

## Freedom of Information Request

---

**Reference Number:** [EPUT.FOI.22.2436](#)  
**Date Received:** [23 March 2022](#)

---

**Information Requested:**Child and Adolescent Mental Health Services (CAMHS)

1. When sexual abuse is disclosed (at any point in assessment/treatment) is there a local policy or a standard way in which this should be recorded (e.g., description within case notes)?
  - a. Do these policies refer to sexual abuse that occurs online (e.g., social media, internet contact made, sharing images)?

Please see attached:

- [CLP37 Safeguarding Children Policy](#)
- [CLPG37 Safeguarding Children Procedure](#)
- [CLPG37 – Appendix 1 – Training Framework for Safeguarding Children](#)
- [CLPG37 – Appendix 4 - Procedure for Responding to Domestic Abuse Domestic Incident Reports](#)
- [CLPG37 – Appendix 5 - Procedure on the Welfare of Unborn Babies](#)
- [CLPG37 Appendix 6 - Procedure for Safeguarding Children in whom Illness is Fabricated or Induced.](#)
- [CLPG37 - Appendix 7 - Procedure for Safe Working Practice with Children - Managing Allegations Against People Who Work with Children](#)
- [CLPG37 - Appendix 8 - Procedure on Child Safeguarding Practice Reviews](#)
- [CLPG37 - Appendix 9 - Procedure for Unexpected Child Death and Learning Disabilities Mortality Review Processes](#)
- [CLPG37 - Appendix 10 - Procedure for Court Appearances & Formal Statements](#)

EPUT has a Safeguarding children policy (CLP37) which complies with the CQC requirements and reflects 'Working together to safeguard Children' document, supports. EPUTs safeguarding children procedure (CLPG37) which stipulates (4.7) sexual abuse may also include non-contact activities. The Trusts child protection procedure provides guidance to staff in section 4 regarding the definition, recognition and indicators of abuse. Specific guidance is referenced in 4.7 to 4.8 on sexual abuse and sexual activity and its legal implications and section 4.9 on Child sexual exploitation and online forms of abuse. EPUT Safeguarding children's procedure ( 4.9.3) explains the term 'E-safety' as ...' process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach including policies and procedures, infrastructures and training. The aim is to reduce the risk of exploitation

through online technologies. The impact of online based sexual abuse for children and young people includes the visual record of the abuse and the sharing of this over the internet re-victimises the victim each viewing. Youth Produced Sexual Imagery or sexting is defined as children under 18 years of age exchanging messages or images with or without consent. Grooming of a child online can include the development of a “special relationship” with the child which remains a secret in preparation for an offline meeting to take place. Abusers may use child sexual abuse images to break down a child’s barriers to sexual behaviours and diminish the child’s inhibitions.’

Guidance on making a referral is accessed in section 6 of the procedure along with advice on recording a disclosure. Guidance is available on the National Assessment Framework to assist practitioners in making their referral. Staff are guided to access relevant e-safety leaflets and information that are available to them and the safeguarding team are members of the area child sexual exploitation sub groups to access the Child Sexual Exploitation toolkits and resources available for staff to guide them with referrals.

There is a clear protocol that identifies that the incident/disclosure is recorded in the records, the safeguarding team contacted and a Datix completed.

2. List all assessment tools that make references to a patient’s online life (i.e., assessment mentioning young people engaging with social media, frequency of use of the internet)
  - a. Indicate if assessment tools ask about:
    - i. Online child sexual exploitation (colloquially referred to as ‘online grooming’) - No
    - ii. Youth-produced sexual image
      1. Sextortion - No
      2. Non-consensual sexual images - No
    - iii. Live streaming - No
    - iv. Abuse through production, dissemination, or possession of child sexual abuse material (videos or images)- No

No assessment tool makes specific reference to online activity. As part of gathering social history it is something we are asked to note. On Mobius the admission assessment form can be attached. The Doctors do ask as part of their admission assessment (Part 1) about abuse. Nurses ask in the initial assessment on Paris. Records have a risk assessment format that includes “Risk of other forms of harm from others” where on a weekly basis, our nursing team would be documenting if there are any concerns with regards to the online life.

3. What support and interventions do you offer to a service user who has experienced technology-assisted sexual abuse?

Please see attached:  
CLPG37 EPUT Safeguarding Children Procedure

CPG50 - Information Governance and Security Procedure  
CPG50b - Email, Intranet, and Internet Access and Use Procedure  
CPG50D - Information Governance Incident Reporting Procedure  
CPG54 - Appendix 1 - Contract for Providing a Mobile Phone Number  
CPG54 - Appendix 2 - Contract for Patient Use of A Mobile Phone

“4.9.4 The Trust has an Executive Director responsible for E-Safety within the Trust. The Trust has a number of policies and procedures aimed to protect staff and service users. These include the IT & T Information Governance & Security Policy “CP50 - Information Governance and Security Policy” and CPG54 - Use of Mobile Phones Policy and are attached which contains risk assessment tools.

4.9.5 Trust sites contain leaflets and information on E-Safety measures for Young people and parents. Young people in Adolescent Mental Health Units have limited access to mobile phones. Computers used in the school room are supervised at all times. However staff should ensure that young people have access to information and resources which aims to keep them safe.”

- a. Is the support or intervention offered specific to technology-facilitated sexual abuse?

Please see attached CLPG37 – Appendix 2 – Procedures for Safeguarding Supervision. The Trust would offer Emotional support, referral to police and safeguarding. We would remove technology or put a system in place to manage access to technology – i.e. safe access via supervision. Liaison and/or referral to Children’s Social Care, depending whether the case is already open to them. As part of the educational curriculum the young people do online safeguarding training. Therapeutic support is available on the unit to all young people. The Trust would involve the family with the young person’s consent, and involve them in the safety plan and the decision making.

4. Is training provided to staff on online harms and the impact of technology-assisted sexual abuse young people?
  - a. If yes, what does the training cover?

All staff working in Tier 4 CAMHS in-patient units are mapped to receive Level 3 safeguarding children training, in line with the intercollegiate document (Safeguarding Children and Young People: Roles and Competencies for Healthcare Staff – RCN, 2019).

The training includes:

1. Specific risks to adolescents.
2. Grooming online and otherwise. Online safety. Traumatic and inappropriate images seen by even young children, online. Cyberbullying.

3. Radicalisation and PREVENT (please see attached CLPG37 - Appendix 11 - Procedure for Prevent)
  4. Child exploitation, including sexual, criminal, online and modern slavery. Definition of CSE.
  5. The particular issues around boys and CSE.
  6. The particular impact of online abuse: i.e. it is just as traumatic as face to face abuse, in some ways worse as the child is unable to avoid the situation, even when they are at home, and effectively are threatened and enslaved in the situation.
  7. Trafficking and NRM notification.
  8. The challenges of contextual safeguarding.
  9. County Lines.
  10. Links to further resources/online training on child exploitation and online safety.
  11. The link between exploitation and young people who go missing, including the importance of return to home interviews and the consideration that missing episodes could be a sign of abuse within the home.
  12. Neglect and adolescence.
  13. The impact of Covid on children's online life.
  14. The changing picture of child grooming and the importance of gaming in this, so that the grooming, which might have been visible previously, in terms of concrete gifts, is now largely invisible, as the gifts are items within the game.
  15. Information and links to CEOP.
  16. Technology Assisted Harmful Sexual Behaviour in young people.
  17. Criminalisation of young people who have been exploited and abused themselves. The use of non-victim blaming language.
  18. Sexual abuse within gang culture.
  19. Peer on peer abuse and grooming.
  20. The training also includes a video, Blurred Lines, showing grooming of a child into County Lines via social media, as well as the use of mobile phones and texting to locate and control young people.
  21. Any further comments. *N/A*
5. SARC
1. Are there policies or a standard way to record technology-assisted sexual abuse when it is disclosed (at any point in assessment/treatment)? *n/a*
    - a. If yes, please list the policies. *n/a*
  2. Are there assessment methods that are used to assess for technology-assisted sexual abuse? *n/a*
    - a. If yes, list the assessment methods that reference the following:
      - i. Online child sexual exploitation (colloquially referred to as 'online grooming') *n/a*
      - ii. Youth-produced sexual image *n/a*
        1. Sextortion *n/a*
        2. Non-consensual sexual images *n/a*
      - iii. Live streaming *n/a*

- iv. Abuse through production, dissemination, or possession of child sexual abuse material (videos or images) *n/a*
- 3. What support and interventions do you offer to a service user who has experienced technology-assisted sexual abuse? *n/a*
  - a. Do these support or interventions involve referral to mental health services? *n/a*
    - i. If yes, are these mental health services located outside or within the NHS system? *n/a*
- 4. Is training provided to staff on online harms and the impact of technology-assisted sexual abuse young people? *n/a*
  - a. If yes, what does the training cover? *n/a*

Essex Partnership University NHS Foundation Trust does not provide services for SARC. Essex SARC is provided by SERCO at Brentwood Community Hospital and is funded by NHSE.

---

**Publication Scheme:**

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT's Publication Scheme is located on its Website at the following link <https://eput.nhs.uk>

## SAFEGUARDING CHILDREN POLICY

<b>POLICY NUMBER:</b>	CLP37
<b>VERSION NUMBER:</b>	2
<b>AUTHOR:</b>	Head of Safeguarding Children
<b>CONSULTATION GROUPS:</b>	Trust Safeguarding Group Mental Health and Safeguarding Sub-Committee
<b>IMPLEMENTATION DATE:</b>	April 2017
<b>AMENDMENT DATE(S):</b>	May 2019
<b>LAST REVIEW DATE:</b>	January 2020
<b>NEXT REVIEW DATE:</b>	January 2023
<b>APPROVAL BY MENTAL HEALTH &amp; SAFEGUARDING SUB-COMMITTEE:</b>	July 2019
<b>APPROVAL BY QUALITY COMMITTEE:</b>	January 2020
<b>COPYRIGHT</b>	2017

<b>POLICY SUMMARY</b>
<p>This policy sets out the roles and responsibilities of Trust staff in working together with other professionals and agencies in promoting children's welfare and safeguarding them from abuse and neglect. This policy complies with the Care Quality Commission requirements and reflects the HM Government: <i>Working Together to Safeguard Children 2018</i> Document the Local Safeguarding Children Board Guidance for Bedfordshire, Suffolk, Southend, Essex, Thurrock, and Pan London, and the principles of the Safeguarding Vulnerable People in the NHS- Accountability and Assurance Framework 2015</p>
<b>The Trust monitors the implementation of and compliance with this policy in the following ways;</b>
<p>Monitoring of implementation and compliance with this policy and associated procedural guideline will be undertaken by the Trust Safeguarding teams and the Mental Health Act and Safeguarding Sub-Committee.</p>

Services	Applicable	Comments
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is  
The Executive Nurse**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**POLICY ON SAFEGUARDING CHILDREN**

**CONTENTS**

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

- 1.0 INTRODUCTION**
- 2.0 SCOPE**
- 3.0 LEGAL FRAMEWORK**
- 4.0 DEFINITIONS**
- 5.0 PARENTS AND CHILDREN WHO ARE BOTH SERVICE USERS**
- 6.0 TRAINING**
- 7.0 SUPERVISION**
- 8.0 CONSENT, CONFIDENTIALITY & INFORMATION SHARING**
- 9.0 RECRUITMENT**
- 10.0 CARE QUALITY COMMISSION (CQC)**
- 11.0 RESPONSIBILITIES**
- 12.0 IMPLEMENTATION**
- 13.0 MONITORING AND REVIEW**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

POLICY ON SAFEGUARDING CHILDREN

**1.0 INTRODUCTION**

- 1.1 The Trust believes that the welfare of children and young people is paramount and at all times and in all situations a child or young person has the right to feel safe and protected from any situation or practice that results in them being harmed or at risk of harm.
- 1.2 This policy sets out the principles of Safeguarding Children and gives guidance to staff on what to do if concerned for the welfare and protection of a child/ren.
- 1.3 This policy applies to those working in mental health and community health settings and contains a number of appendices which staff should read in conjunction with Local Safeguarding Partnership guidance from;
- Bedfordshire <http://bedfordscb.proceduresonline.com/index.htm>
  - Luton [www.lutonlscb.org](http://www.lutonlscb.org)
  - Southend, Essex & Thurrock (SET) [www.escb.org.uk](http://www.escb.org.uk).
  - Suffolk [www.suffolkscb.org.uk](http://www.suffolkscb.org.uk)
  - Pan London [www.londoncp.co.uk](http://www.londoncp.co.uk)
- 1.4 All National, Local and EPUT policies, guidance and protocols are available on the trust Safeguarding Intranet site.
- 1.5 This policy has been developed in line with the Trust principles of Equality and Diversity and is underpinned by the following standards:
- The child's needs come first regardless of who is the primary Trust client;
  - The child's welfare and safety is everyone's responsibility;
  - Staff must work together, understand and appreciate other professionals roles and responsibilities;
  - No one must be discriminated against on the grounds of age, ethnicity, religion, culture, class, sexual orientation, gender or disability.
- 1.6 Where English may not be the first language the Trust interpreter services, or those services to meet a child or parent's communication needs must be accessed and details recorded in case notes.

**2.0 SCOPE**

- 2.1 This policy applies to all employees (permanent or temporarily) and volunteers of the Trust and those people that perform work on behalf of the Trust.
- 2.2 This policy complements all professional or ethical rules, guidelines and codes of professional conduct on child protection. (E.g. Nursing & Midwifery Code of Professional Conduct, General Social Care Council, and General Medical Council).

### 3.0 LEGAL FRAMEWORK

- 3.1 The Government document, *Working Together to Safeguard Children 2018* refers to a child or young person as a person up to their 18<sup>th</sup> birthday.
- 3.2 The Children Act (1989/2004) makes it clear that Safeguarding Children is **everyone's** responsibility. It imposes a duty on the Trust to ensure that its functions are discharged with regard to the need to safeguard and promote the welfare of children as per Section 11 of the Children Act 2004 and to assist Local Authorities in carrying out enquiries into whether or not a child is at risk of significant harm (Section 47). It also requires the Trust to take part in Local area Safeguarding Partnership Arrangement functions and duties.
- 3.3 *Working Together to Safeguard Children (2018)* states that;
- Everyone who works with children has a responsibility for keeping them safe
  - Health Professionals are in a strong position to identify welfare needs or safeguarding concerns regarding individual children and, where appropriate, provide support.
  - Effective Safeguarding of children can only be achieved by putting children at the centre of the system, and by every individual and agency playing their part, working together to meet the needs of our most vulnerable children.
  - For services to be effective they should be based on a clear understanding of the needs and views of children
- 3.4 Staff are required to co-operate with police and the Local Authority when approached for a formal statement or a request to attend court as a witness. In these circumstances staff must inform the relevant Safeguarding Team and their line manager. Appendix 10 of the Procedures gives further advice, guidance and support for Trust staff.

### 4.0 DEFINITIONS

- 4.1 The DoH *Working Together to Safeguard Children 2018* defines safeguarding children as;
- 'protecting children from maltreatment, preventing impairment of health or development, ensuring that children are growing up in circumstances consistent with the provision of safe and effective care and taking action to enable all children to achieve their best outcomes'*
- 4.2 **Child Protection**  
Child Protection refers to the activity that is undertaken to protect children where there is reasonable cause to suspect a child/ren is suffering or is likely to suffer significant harm.
- 4.3 **Significant Harm**  
The Children Act 1989 (Section 47) introduced the concept of significant harm as the threshold that justifies compulsory intervention in family life in the best interests of the child and gives local authorities a duty to make enquiries to decide whether they should take action to safeguard and promote the welfare of a child suffering or likely to

## CLP37 - SAFEGUARDING CHILDREN POLICY

suffer significant harm. In addition harm is defined as the ill treatment or impairment of health and development.

4.3.1 Significant harm relates to four categories of abuse. These are physical, emotional, sexual abuse and neglect.

4.3.2 Working Together to Safeguard Children further describes exploitation by criminal gangs, organised crime groups, trafficking, online abuse, sexual exploitation, and the influences of extremism leading to radicalisation.

4.3.3 Where Trust staff are aware that a child has suffered or is at risk of suffering significant harm, a referral to Children's Social Care **must** be made.

4.3.4 The referral is an outcome of staff concerns for a child/ren and as such an incident should be also be raised via the Trust DATIX system for risk management purposes with the referral attached within the Datix form.

### 4.4 Contextual Safeguarding

4.4.1 Contextual Safeguarding is an approach to understanding and responding to young people's experiences outside of their families. It acknowledges the relationships that young people can form in school, online and in their community and how these can feature violence and abuse. Their parents and carers can have little influence over these context and young people's experiences of inter-familiar abuse can undermine the parent-child relationship. Contextual Safeguarding therefore widens the child protection system to include the recognition that young people may be vulnerable to abuse in a range of social contexts.

### 4.5 Children in Need

4.5.1 Local Authorities have a duty to safeguard and promote the welfare of children in need

4.5.2 Children who are defined as being 'in need' under Section 17 of the Children Act 1989 are those whose vulnerability is such that they are unlikely to reach or maintain a satisfactory level of health or development without the provision of services. This includes those children who are disabled and have specific additional needs.

### 4.6 Early Help

4.6.1 Providing early help is more effective in promoting the welfare of children than reacting later. Early help means providing support as soon as a problem emerges, at any point in a child's life, from the foundation years through to the teenage years. Practitioners should be alert to the potential need for early help for a child who:

- Has special education needs regardless of a Statutory Education Health Care Plan.
- Is disabled and has specific additional needs
- Is a young carer

- Is showing signs of anti-social or criminal behaviour
- Is frequently missing from care/home
- Is at risk of modern slavery, trafficking or exploitation
- At risk of being radicalised
- Are misusing drugs or alcohol
- Are within family circumstances facing challenges such as drug and alcohol misuse, parental mental health issues and domestic abuse
- Is a privately fostered child or returned home from care
- Has returned home to their family from care
- Is showing early signs of abuse or neglect

4.6.2. Effective early help relies upon local agencies working together to:

- Identify children and families who would benefit from early help;
- Undertake an assessment of the need for early help by the Lead Practitioner; and
- Provide targeted early help services to address the assessed needs of a child and their family which focuses on activity to significantly improve the outcomes for the child.

### 4.7 Looked After Children

4.7.1 The term Looked After Child (LAC) was introduced by the Children Act 1989 and refers to children who are subject to care orders or voluntary accommodated. The Local Authority has responsibility for Looked After Children.

4.7.2 Looked After Children have often experienced abuse or neglect and will have additional health care needs. The Local Authority has a statutory responsibility to ensure the health care needs of children and young people are being assessed. Community Health Services work closely with the Local Authority to ensure that health care plans set out how identified health needs will be addressed.

4.7.3 For detailed information on LAC procedures, staff should refer to the specific protocol in their area and refer to the Local Safeguarding partnership arrangement guidance accordingly.

## 5.0 PARENTS AND CHILDREN WHO ARE BOTH SERVICE USERS

5.1 It is important that consideration be given to a co-ordinated 'Think Family' approach and partnership working, where it is identified that both a parent and their child/ren are service users.

5.2 Staff who work directly with children should ensure that safeguarding and promoting their welfare forms an integral part of all stages of care and services offered. Staff who come into contact with children, parents and carers in the course of their work need to be aware of their safeguarding responsibilities and be able provide preventative support through proactive work.

## CLP37 - SAFEGUARDING CHILDREN POLICY

- 5.3 Where a child and parent are both known to be receiving a service from the Trust, staff including doctors from both adult and child services should discuss cases and consider a joint assessment and support plan where appropriate.

### 6.0 TRAINING

- 6.1 All safeguarding and looked after children training will comply with the standards and requirements set by the:
- DoH Intercollegiate Document *Safeguarding Children and Young People: Roles & Competencies for Health Care Staff (2019)* and *Working Together (2018)*.
  - Local Safeguarding Partnership arrangements for Children's Training strategies. Further details are contained within the accompanying Procedures (Appendix 1).
- 6.2 The Trust Safeguarding Training Strategy outlines the requirement that **all** Trust staff must receive Safeguarding Adult and Children Training every three years. Level of training required is dependent on Trust staff role, specialism and contact with service user. Staff must access training within 3 months of starting their post.
- 6.3 Compliance for all safeguarding training is set at 95% of the total of staff. Compliance is discussed at all senior management meetings and the Trust Safeguarding Meeting each month.
- 6.4 Some staff working directly with children will also require supplementary Looked after Children training relevant to their role. The training is competency based and is mapped against the Intercollegiate Framework for Looked after Children (2015).

### 7.0 SUPERVISION

- 7.1 All clinical staff must attend supervision in accordance with the Trust Supervision and Appraisal Policy (HR48) and further details for Safeguarding Children Supervision are detailed within the procedural guidelines (Appendix 2)
- 7.2 Specific Safeguarding Supervision is available from members of the Safeguarding Team in accordance to local protocols.
- 7.3 A record of supervision attendance should be maintained by staff and made available for audit purposes.

### 8.0 CONSENT, CONFIDENTIALITY & INFORMATION SHARING

- 8.1 The Department for Children, Schools and Families (DCSF) and the DoH guidance on the duties of doctors and other health professional's states.

*'When investigating allegations of child abuse or assessing injuries or symptoms which may arise from child abuse, professionals first duty should be owed to the child They should not be distracted from that duty by a parallel duty to anyone else including the parents or carers' (2007)*

- 8.2 The welfare of the child is paramount and staff have a duty to pass on information relating to (Sec 47 Children Act 1989) suspected child abuse to Children's Social

## CLP37 - SAFEGUARDING CHILDREN POLICY

Care. Staff should clarify with Social Care if consent from the parent or child (where appropriate) has been obtained in order to share information. Staff should also clarify with Social Care the exact nature of the information required.

8.3 Consent from a parent or child is **not** required where;

- Seeking permission is likely to increase risk to children;
- Place an adult at risk of serious harm
- Permission has been refused but sufficient professional concern remains to justify disclosure;
- Seeking permission is likely to impede a criminal investigation.

8.4 Guidance is similar for Trust Doctors and Consultants. The General Medical Council (GMC) guidance on '*Confidentiality Protecting and Providing Information*' (2009) is clear that information may be released without consent to 3<sup>rd</sup> parties e.g. Children's Social Care, Police in circumstances where:

- Failure to disclose information may expose the patient or others to risk of death or serious harm;
- 3<sup>rd</sup> parties may have direct relevance to child protection e.g. adults who may pose a risk to children;
- A child/ren who may be the subject of abuse.

8.5 Staff should consult their Line Manager, or a member of the Safeguarding Team for advice.

### 9.0 RECRUITMENT

9.1 The Trust is required to comply with the Disclosure and Barring Service (DBS) which aims to ensure that unsuitable people do not work with children on a paid or voluntary basis.

9.2 All Trust staff working with children and adults will undergo a DBS check. Procedures are contained within the Human Resources Policy (HR28). The Executive Director of People and Culture is responsible for ensuring compliance.

9.3 All job descriptions for new staff contain a statement regarding staff responsibility for adhering to Trust policies on Safeguarding children and adults.

### 10.0 CARE QUALITY COMMISSION (CQC)

10.1 Any Child Safeguarding Practice review, formally known as a Serious Case Review, agreed by the Local Safeguarding Partnership arrangements which involves a child or family known to the Trust will be reported to the Designated Nurse for Safeguarding Children in the appropriate CCG. The CCG will inform NHS England Midlands & East or who will inform the CQC within one month of notification

## 11.0 RESPONSIBILITIES

- 11.1 **Chief Executive Officer** - To raise the profile, support the policy, and promote the development of initiatives to ensure the protection of children.
- 11.2 **Executive Nurse** – Is the Trust Board Executive Lead for Safeguarding children and adults and takes responsibility for governance systems and the organisational focus on safeguarding. The Executive Director represents the Trust at Local Safeguarding Partnership arrangements and is the Chair of the Trust Mental Health Act and Safeguarding Sub-committee.
- 11.4 **Executive Medical Director** – Is the Trust Named Senior Officer for managing allegations against staff.
- 11.3 **Trust's Named Professionals (Doctor, Nurse, Specialist Practitioner)**
- 11.3.1 Named professionals have a key role in promoting good professional practice and providing advice and expertise for staff. They support the Clinical Governance role within the Trust by ensuring audits and training is undertaken and Safeguarding issues are integrated into Clinical Governance Systems.
- 11.3.2 Named Professionals will provide regular reports to the Trust Committees.
- 11.3.3 Named Professionals and relevant senior staff are responsible for linking with the Local Safeguarding Partnership arrangements to share information and provide specialist advice to those networks in respect of services or information provided by the Trust.
- 11.4 **Managers**
- 11.4.1 Managers will be responsible for ensuring that staff are equipped and supported in dealing with Safeguarding concerns.
- 11.4.2 Managers are responsible for ensuring staff attend the correct level of Safeguarding training and supervision according to role and with the appropriate, signed study leave form completed in accordance with the Training Strategy.
- 11.4.3 Managers should support those staff working with families where there are Safeguarding concerns and following a child safeguarding practice review regarding decision making and monitoring of actions.
- 11.4.4 Managers should ensure Safeguarding issues are routinely addressed during supervision and ensure that actions are carried through.
- 11.4.5 Managers should discuss staff safeguarding competencies during annual appraisal with staff and identify any training or development needs required.

**11.5 All staff**

All staff must be aware of and follow the legislation, and guidance regarding Child Protection and Safeguarding Children as stated in these and the Local Safeguarding Partnership arrangements. This includes accessing training and updates of Safeguarding matters.

**12.0 IMPLEMENTATION**

- 12.1 The Executive Directors, Clinical Directors and Service Directors are responsible for implementing this policy and the associated procedural guidelines.
- 12.2 All clinical areas will have access to these policies, procedural guidance and the Local Safeguarding Partnership arrangement Procedures via Trust Intranet Safeguarding site.

**13.0 MONITORING & REVIEW**

- 13.1 The Executive Nurse will be responsible for the overall monitoring and review of this policy.
- 13.2 This policy will be reviewed every three years.
- 13.3 An audit of key parts of this policy will be undertaken every three years with a rotating theme, for example; recommendations from Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews, Referral process to Social Care, training uptake.

**END**

## SAFEGUARDING CHILDREN PROCEDURE

<b>PROCEDURE NUMBER:</b>	CLPG37
<b>VERSION NUMBER:</b>	2
<b>AUTHOR:</b>	Head of Safeguarding Children
<b>CONSULTATION GROUPS:</b>	Trust safeguarding team, Mental Health Act and Safeguarding Sub-Committee
<b>IMPLEMENTATION DATE:</b>	April 2017
<b>AMENDMENT DATE(S):</b>	May 2019
<b>LAST REVIEW DATE:</b>	January 2020
<b>NEXT REVIEW DATE:</b>	January 2023
<b>APPROVAL BY MENTAL HEALTH &amp; SAFEGUARDING SUB-COMMITTEE:</b>	July 2019
<b>APPROVAL BY QUALITY COMMITTEE:</b>	January 2020
<b>COPYRIGHT</b>	2017

<b>POLICY SUMMARY</b>
<p>These procedural guidelines will enable staff to recognise and take appropriate action when there is a concern or allegation of significant harm to child/ren. The procedure complies with Working Together to Safeguard Children 2018, Guidance from the Local Safeguarding Partnership arrangements in Essex, Bedfordshire, Suffolk, Pan London and reflects the principles of the Safeguarding Vulnerable People in the NHS- Accountability and Assurance Framework 2015.</p> <p>These procedures also reflect local Trust children's services operational protocols available on the Trust Intranet page</p>
<b>The Trust monitors the implementation of and compliance with this policy in the following ways;</b>
<p>Monitoring of implementation and compliance with this policy and associated procedural guideline will be undertaken by the Mental Health Act and Safeguarding Sub-Committee.</p>

### SCOPE

Services	Applicable	Comments
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is the Executive Nurse**

PROCEDURAL GUIDELINES FOR SAFEGUARDING CHILDREN

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

- 1.0 INTRODUCTION
- 2.0 REPORTING TO THE CARE QUALITY COMMISSION (CQC)
- 3.0 INCIDENT REPORTING
- 4.0 DEFINITION, RECOGNITION & INDICATORS OF CHILD ABUSE
- 5.0 RISK FACTORS
- 6.0 PROCEDURE: WHERE THERE ARE CONCERNS THAT A CHILD/REN HAS SUFFERED OR IS LIKELY TO SUFFER SIGNIFICANT HARM
- 7.0 RECORD KEEPING
- 8.0 ACCESS TO INFORMATION
- 9.0 MISSED APPOINTMENTS, NON COMPLIANCE & HOSTILE CARERS
- 10.0 HISTORICAL ABUSE ALLEGATION
- 11.0 VULNERABILITY, COMPLEX FACTORS & ADDITIONAL NEEDS
- 12.0 EARLY HELP ASSESSMENT (EHA)
- 13.0 IMPLEMENTATION
- 14.0 MONITORING & REVIEW

<b>APPENDICES</b>
-------------------

**APPENDIX 1 – TRAINING FRAMEWORK FOR SAFEGUARDING CHILDREN & ADULTS**

**APPENDIX 2 – PROCEDURES FOR SAFEGUARDING SUPERVISION**

**APPENDIX 3 – PROCEDURE ON CHILD PROTECTION CONFERENCES**

**APPENDIX 4 – PROCEDURE FOR RESPONDING TO DOMESTIC ABUSE AND DOMESTIC INCIDENT REPORTS**

**APPENDIX 5 – PROCEDURE ON THE WELFARE OF UNBORN BABIES**

**APPENDIX 6 – PROCEDURE FOR SAFEGUARDING CHILDREN IN WHOM ILLNESS IS FABRICATED OR INDUCED**

**APPENDIX 7 – PROCEDURAL GUIDELINES FOR SAFE WORKING PRACTICE WITH CHILDREN & MANAGING ALLEGATIONS AGAINST PEOPLE WHO WORK WITH CHILDREN**

**APPENDIX 8 – PROCEDURE ON CHILD SAFEGUARDING PRACTICE REVIEWS**

**APPENDIX 9 – PROCEDURE FOR UNEXPECTED CHILD DEATH AND NATIONAL LEARNING DISABILITIES MORTALITY REVIEW PROCESSES**

**APPENDIX 10 – PROCEDURE FOR COURT APPEARANCES & FORMAL STATEMENTS**

**APPENDIX 11 – PROCEDURE FOR PREVENT**

### 1.0 INTRODUCTION

- 1.1 Safeguarding is everyone's responsibility and as such the Trust is committed to Safeguarding and promoting the welfare of children and young people. A child is defined as those up to their 18<sup>th</sup> birthday and it is the responsibility of all Trust staff to follow these procedures and the associated policy to safeguard children regardless of which member of the family is the primary service user.
- 1.2 These procedural guidelines provide the knowledge base and guidance on what actions to take when there are concerns, allegations or disclosures of actual harm or risk of harm to a child/ren. The appendices outlined below provide additional information on key statutory guidance outlined in DoH *Working Together to Safeguard Children 2018*.
- 1.3 Staff should follow these overarching procedures but note that there are also a number of local Operational Protocols that may be relevant for specific areas. These should also be referred to where required and are available on the Trust intranet. Members of the Safeguarding Team are available for advice, support and assistance for any Safeguarding matter.
- 1.4 These procedural guidelines and the associated policy should be read in conjunction with the Local Safeguarding Partnership arrangement procedures of areas staff may work in.
- Bedfordshire <http://bedfordscb.proceduresonline.com/index.htm>.
  - Luton [www.lutonlscb.org](http://www.lutonlscb.org)
  - Southend, Essex & Thurrock (SET) [www.escb.org.uk](http://www.escb.org.uk)
  - Suffolk [www.suffolkscb.org.uk/](http://www.suffolkscb.org.uk/)
  - Pan London [www.londonscb.gov.uk/procedures](http://www.londonscb.gov.uk/procedures)
- 1.5 Where English is not the first language, the Trust interpreter services must be accessed, and the services to meet a child or parents communication needs and details recorded in case notes.

### 2.0 REPORTING TO THE CARE QUALITY COMMISSION (CQC)

- 2.1 The Care Quality Commission is the independent regulator of health and adult social care services in England. The CQC has a set of essential levels of safety and quality to be maintained.
- 2.2 The Trust reports on all Local Child Safeguarding Practice reviews formally known as Serious Case Reviews, Domestic Homicide Reviews, and safeguarding referrals to the CQC via the Local Safeguarding Partnership arrangements and Designated Nurse within the Clinical Commissioning Group (CCG). (Appendix 8 Local Child Safeguarding Practice Reviews).

### 3.0 INCIDENT REPORTING

- 3.1 Any serious Incident, (Adverse Incident Policy CP3) deaths or child protection (Sec.47) referrals to Social Care involving children must be reported to the Trust Integrated Risk Department via DATIX.
- 3.2 Child Deaths are also reported to the Local Child Death Review Administrator (see Appendix 9)
- 3.3 A weekly meeting between the Serious Incident and Safeguarding team takes place to share information and ensure consistent notification and processing of Serious Incidents that involve a safeguarding issue.

### 4.0 DEFINITION, RECOGNITION & INDICATORS OF CHILD ABUSE

- 4.1 Concerns for a child's welfare may arise when a member of staff is not entirely satisfied with the clinical, social or emotional picture that is presented or where abuse is suspected.
- 4.2 The Children Act 1989 (Section 47) introduced the concept of significant harm as a definition of abuse;
  - Harm means ill treatment or the impairment of health or development, including for example, impairment suffered from seeing or hearing the ill-treatment of another e.g. domestic abuse;
  - Significant relates to the child's health and development and the comparison with that which could reasonably be expected of a similar child.
- 4.3 Significant harm relates to four categories of abuse, these are physical, emotional, sexual abuse and neglect.
- 4.4 **Physical abuse**

Physical abuse includes any form of abuse which may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating, female genital mutilation or otherwise causing physical harm to a child. Physical harm may also be caused when a parent or carer fabricates the symptoms of, or deliberately induces, illness in a child. (Appendix 6 gives further guidance).

Bruising/injury to an immobile baby must be referred to Children's Social Care, with the expectation that a Child Protection Medical will be undertaken. Further guidance is available within the SET Multi Agency Management of Suspicious / Unexplained Injuries / Bruising in Children Protocol, 2018 which is available on the Trust Intranet site.

Any bruise/mark on a child should be considered in light of the history provided; location of the bruise/mark; and the age and developmental stage of the child/infant. If the child is under 6 months of age; not independently mobile; or under 18 years of age and there is suspicion of non-accidental injury; the professional must refer the child/family into Children's Social Care, following the Local Child Protection and Safeguarding Procedures.

If the child/infant is under 6 months of age, and/or immobile, Health/Medical professionals may use the pre-assessment tool on the Trust Intranet site to assist in an assessment of the bruise/mark. If in any doubt the professional must refer the child/family into Children's Social Care, following local area procedures.

### 4.5 Emotional Abuse

Emotional abuse is the persistent emotional maltreatment of a child such as to cause severe and persistent adverse effects on the child's emotional development. It may involve conveying to a child that they are worthless or unloved, inadequate, or valued only in so far as they meet the needs of another person. It may include not giving the child opportunities to express their views, deliberately silencing them or 'making fun' of what they say or how they communicate. It may feature age or developmentally inappropriate expectations being imposed on children. These may include interactions that are beyond a child's developmental capability, as well as overprotection and limitation of exploration and learning, or preventing the child participating in normal social interaction. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyber bullying), causing children frequently to feel frightened or in danger, or the exploitation, radicalisation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, though it may occur alone.

### 4.6 Neglect

Neglect is the persistent failure to meet a child's basic physical and/or psychological needs, likely to result in the serious impairment of the child's health or development. Neglect may occur during pregnancy as a result of maternal substance abuse. Once a child is born, neglect may involve a parent or carer failing to:

- provide adequate food, clothing and shelter (including exclusion from home or abandonment)
- protect a child from physical and emotional harm or danger
- ensure adequate supervision (including the use of inadequate care-givers)
- ensure access to appropriate medical care or treatment

It may also include neglect of, or unresponsiveness to, a child's basic emotional needs.

### 4.7 Sexual Abuse

Sexual abuse Involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example, rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing.

Sexual abuse may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, child sexual exploitation, grooming a child in preparation for abuse including via the internet or the use of technology. Sexual abuse can be perpetrated by men, women or other children. Sexual abuse should be considered for those children who run away from home. Pregnancy in a young person or a concealed pregnancy may also raise concerns of sexual abuse.

### 4.8 Sexual Activity and Legal Implications

Cases of underage sexual activity that present a cause for concern should be handled sensitively and staff should seek advice where required. The Law clearly states that;

#### 4.8.1 Under 13 years

Sexual activity with a child under 13 years is a criminal offence as the child is not legally capable of consenting to sexual activity (Sexual Offences Act 2003). Trust staff must report any known cases to their line manager, the Trust Safeguarding Team. Such cases must always be referred to Children's Social Care or police.

#### 4.8.2 Age 13 - 15

Sexual activity with a child under 16 is an offence. Where it is consensual it may be less serious than if the child were under 13 but may nevertheless have serious consequences for the welfare of the young person. Staff should seek advice when they are concerned.

#### 4.8.3 Age 16 – 17

It is an offence for a person to have a sexual relationship with a 16-17 year old if that person holds a position of trust or authority in relation to them e.g. teacher, doctor, Nurse. Staff must report any known cases to their line manager, the Trust Safeguarding Team and be referred to Children's Social Care or the police.

### 4.9 Child Sexual Exploitation (CSE) and Online based forms of abuse (E-Safety)

4.9.1 Information communication technology is a medium for a wide range of abuse and exploitation for physical, sexual and emotional abuse including bullying via mobile telephones or online (Internet) with verbal and visual messages. The sexual exploitation of children and young people involves exploitative situations, contexts and relationships where young people (or a third person or persons) receive 'something' (for example, food, accommodation, drugs, alcohol, cigarettes, affection, gifts, money) as a result of performing, and or others performing on them, sexual activities. It is a form of sexual abuse and occurs when an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive the child.

4.9.2 Child sexual exploitation can occur through use of technology without the child's immediate recognition, for example the persuasion to post sexual images on the internet/mobile phones with no immediate payment or gain. In all cases those exploiting the child/young person have power over them by virtue of their age, gender, intellect, physical strength and /or economic or other resources." The victim may have been sexually exploited even if the sexual activity appeared to be consensual. Exploited children should be treated as victims of abuse, not as offenders.

4.9.3 The term **E-safety** is the process of limiting the risks to children and young people when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach including policies and procedures, infrastructures and training. The aim is to reduce the risk of exploitation through online technologies. The impact of online based sexual abuse for children and young people includes the visual record of the abuse and the sharing of this over the internet re-victimises the victim each viewing. Youth Produced Sexual Imagery or sexting is defined as children under 18 years of

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

age exchanging messages or images with or without consent. Grooming of a child online can include the development of a “special relationship” with the child which remains a secret in preparation for an offline meeting to take place. Abusers may use child sexual abuse images to break down a child’s barriers to sexual behaviours and diminish the child’s inhibitions.

4.9.4 The Trust has an Executive Director responsible for E-Safety within the Trust. The Trust has a number of policies and procedures aimed to protect staff and service users. These include the IT & T Information Governance & Security Policy CP50 and Mobile Phone policy CP54 which contains risk assessment tools.

4.9.5 Trust sites contain leaflets and information on E-Safety measures for Young people and parents. Young people in Adolescent Mental Health Units have limited access to mobile phones. Computers used in the school room are supervised at all times. However staff should ensure that young people have access to information and resources which aims to keep them safe.

4.9.6 The Trust are active members of Strategic Child Sexual Exploitation groups In Essex, Southend and Bedford and contribute toward the development of CSE Toolkits and other resources to help staff respond to concerns and service users in gaining knowledge and support. The Trust Intranet Safeguarding site offers more information and advice such as the Child Exploitation and Online Protection Centre. <http://www.ceop.police.uk> and Childnet International website <http://www.childnet-int.org/>

### 4.10 Criminal Exploitation, County Lines and Cuckooing

4.10.1 **Child Criminal Exploitation** occurs where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child or young person under the age of 18. The victim may have been criminally exploited even if the activity appears consensual. Child Criminal Exploitation does not always involve physical contact; it can also occur through the use of technology. Criminal exploitation of children includes for instance children forced to work on cannabis farms or to commit theft. (Home Office 2018)

4.10.2 Criminal exploitation involves taking advantage of vulnerable people, often the very young, the impoverished or the infirm. Forcing them to engage in various forms of criminal activity such as begging, pick-pocketing, credit card, benefit fraud and the cultivation of cannabis for drug dealers. The Home Office (2017) describes the Criminal Exploitation (CE) of children and vulnerable adults as “a geographically widespread form of harm that is a typical feature of County Lines activity”. **County Lines** is the term used by the police for urban gangs that supply drugs to suburban areas as well as market and coastal towns through the use of dedicated mobile lines referred to as “deal lines”.

4.10.3 County lines is about modern slavery, human trafficking and exploitation, alongside drug supply and violent crime. County lines may involve the commission of the offences of ‘slavery, servitude and forced or compulsory labour’ and ‘human trafficking’ as defined by the Modern Slavery Act 2015. Children’s travel may be ‘arranged and facilitated by a person, with the view to them being exploited’, which amounts to human trafficking according to section 2 of the Modern Slavery Act 2015. Children may then be forced to work for the drug dealer, often held in the vulnerable

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

adult's home against their will and under the force of threat if they do not do as they are told. This meets the definition of 'slavery, servitude and forced or compulsory labour' in section 1 of the Modern Slavery Act 2015.

4.10.4 The **definition of a gang** tends to fall into three categories Peer Groups, Street Gangs and Organised Crime Groups. It can be common for groups of children and young people to gather together in public places to socialise. Although some peer group gatherings can lead to increased antisocial behaviour and youth offending, these activities should not be confused with the serious violence of a street gang. A street gang can be described as a relatively durable, predominantly street-based group of children who see themselves (and are seen by others) as a discernible group for whom crime and violence is integral to the group's identity. An Organised criminal group is a group of individuals normally led by adults for whom involvement in crime is for personal gain (financial or otherwise). This involves serious and organised criminality by a hard core of violent gang members who exploit vulnerable young people and adult.

4.10.5 The criminal exploitation of children includes a combination of:

- **Pull factors:** children performing tasks for others resulting in them gaining accommodation, food, gifts, status or a sense of safety, money or drugs; often the hook is through the perpetrator supplying Class B drugs such as cannabis to the child or young person;
- **Push factors:** children escaping from situations where their needs are neglected and there is exposure to unsafe individuals, where there is high family conflict or the absence of a primary attachment figure;
- **Control:** Brain washing, violence and threats of violence by those exploiting the child particularly when the child or young person is identified by the police, they are expected to take full responsibility for the offences for which they are charged – i.e. possession and supply of illegal substances.

4.10.6 Child Criminal Exploitation occurs as a result of gangs/groups using children or vulnerable people to distribute drugs and money. A base is established in the local area typically taking over the home of a vulnerable adult by force or coercion referred to as **Cuckooing**. Children may be sent to another area of the country to live with a vulnerable adult whose home has been taken over by the gang in exchange for a continued supply of drugs referred to as 'cuckooing'. It can affect both vulnerable adults and children and the activity may appear consensual. It is perpetrated by individuals, groups, males and females and young people or adults. There is typically a form of power imbalance which favours those perpetrating the exploitation and the power imbalance can be as a result of gender, cognitive ability, physical strength, status and available access to economic or other resources.

4.10.7 A key part of the exploitation is the presence of an exchange which could be carrying drugs in return for something. Children as young as 12 years old have been exploited by gangs/groups to courier drugs but the common age range is 15-16. Social media is used to make contact with young people and Class A drug users are targeted in order to take over their home for supply (cuckooing).

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

4.10.8 Some young people are more vulnerable to being exploited as a result of their vulnerability and this includes:

- Those who have experienced neglect, physical and or sexual abuse.
- Being in Care particularly those in residential homes
- Having mental health or substance misuse issues
- Having physical or learning disabilities
- Homeless or insecure accommodation
- Connections with other people involved in gangs
- Living in a chaotic and dysfunctional household.
- Attending school or being friends with young people who are sexually or criminally exploited
- Unsure about their sexual orientation or unable to disclose sexual orientation to their family
- Accompanied or unaccompanied migration or those that have been trafficked into the country

4.10.9 Staff should be alert to the indicators that a young person may be being exploited and any sudden changes in their lifestyle may be an indicator. Indicators of county liners and exploitation involvement are:

- Persistent missing episodes from school or home or found to be out of area.
- Sudden unexplained appearance of money, clothes or mobile phones.
- Excessive receipt of texts or phone calls
- Relationships with controlling/ older individuals or groups
- Suspicion of physical assault/ unexplained injuries
- Carrying a weapon
- Significant decline in school performance
- Self-harming and isolation from peer and social networks

Any staff member that is concerned that a young person may be being exploited should follow the local safeguarding procedures for referral to social care. Advice and support is available from line managers and the Trust Safeguarding team. Staff should evaluate and record their concerns using the local assessment templates for CSE risk and vulnerabilities and make the appropriate referrals for support or protection as required.

### **4.11 Modern day slavery**

4.11.1 The Government introduced the Modern Slavery Bill in March 2015. This recognises that modern slavery is one of the world's largest crime industries and the scale in the UK is significant, affecting adults and children under 18 years.

4.11.2 Modern Slavery can take many forms and involves a whole range of types of exploitation, many of which occur together. These include but are not limited to:

- Trafficking of children
- Sexual exploitation
- Domestic Servitude
- Forced Labour

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

- Criminal exploitation
- Other forms of exploitation e.g. begging, forced marriage
- Drug dealing- most often linked to County Lines and drug mules or decoys
- Credit card and benefit fraud

4.11.3 Traffickers and slave masters use whatever means they have at their disposal to coerce, deceive and force individuals into a life of abuse, servitude and inhumane treatment. Trafficking is often an integral part of exploitation and should therefore be considered when identifying, assessing and responding to all forms of exploitation. Trafficking is the “act of recruitment, transportation, transfer, harbouring or receipt of persons by the means of the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or of position of vulnerability or of the giving/receiving of payments or benefits to achieve the consent of having control over another person”

4.11.4 Children (those aged under 18) are considered victims of trafficking, whether or not they have been coerced, deceived or paid to secure their compliance. They need only have been recruited, transported, received or harboured for the purpose of exploitation.

4.11.5 From November 1<sup>st</sup> 2015 police and Local Authorities have a ‘**duty to notify**’ the Home Office of any one they believe is subject to slavery or human trafficking.

4.11.6 If staff have concerns or suspect slavery then a referral to social care must take place. Consent of the young person will not be required and staff should consult with the Trust Safeguarding team to discuss notifying police.

### 4.12 Female Genital Mutilation (FGM)

4.12.1 Female Genital Mutilation is a severe form of child abuse and violence against women. It comprises all procedures involving partial or total removal of the external female genitalia or other injury to the female genital organs for non-medical reasons.

The practice causes severe pain and has several immediate and long-term health consequences, including difficulties in childbirth also causing dangers to the child

4.12.2 FGM is illegal in the UK and it is illegal to take or assist a person travelling abroad for the purposes of FGM

4.12.3 The procedure may be carried out when the girl is new born, during childhood or adolescence, just before marriage or during the first pregnancy. However, the majority of cases of FGM are thought to take place between the ages of 5 and 8 and therefore girls within that age bracket are at a higher risk.

It is believed that FGM happens to British girls in the UK as well as overseas (often in the family’s country of origin). Girls of school age who are subjected to FGM overseas are thought to be taken abroad at the start of the school holidays, particularly in summer, in order for there to be sufficient time for her to recover before returning to her studies.

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

4.12.4 For families where there is good reason to suspect a child under 18yrs is at risk of FGM a safeguarding children referral to Social Care must be made and the Safeguarding Team should be contacted.

4.12.5 It is mandatory for all staff to report any concerns regarding FGM to a member of the Safeguarding team and record FGM or those at risk of FGM within the service user's records. The Trust records all reports of FGM on the enhanced data set system specific to NHS services.

4.12.6 Staff working in Adolescent Mental Health units must consider FGM as part of initial assessments

4.12.7 The Trust Safeguarding as well as Local Safeguarding partnership arrangement intranet sites contains additional advice & support for staff and service users.

### 4.13 Extremism

4.13.1 Extremism goes beyond terrorism and includes people who target the vulnerable – including the young – by seeking to sow division between communities on the basis of race, faith or denomination; justify discrimination towards women and girls; persuade others that minorities are inferior; or argue against the primacy of democracy and the rule of law in our society.

4.13.2 Extremism is defined in the Counter Extremism Strategy 2015 as the vocal or active opposition to our fundamental values, including the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of our armed forces as extremist.

4.13.3 Radicalisation is the process by which people come to support terrorism and violent extremism and sometime to participate in terrorist groups. There is no profile of a person likely to become involved in extremism and the process of radicalisation is different for every individual. Potential indicators include:

- Use of inappropriate language and the expression of extremist views
- Possession of extremist literature
- Association with known extremists and seeking to recruit others to ideology
- Advocating violent actions and means

## 5.0 VULNERABILITY & RISK FACTORS

5.1 There are certain factors and situations that may place children at particular risk of suffering significant harm. The presence of one or more of these factors does not automatically imply that abuse will result, but may increase the likelihood.

5.2 Staff should be aware of the vulnerability and risk factors for children living with a parent or carer with mental illness, learning disabilities, substance misuse, or in an environment where there is domestic abuse.

### 5.3 Mental Illness

5.3.1 The majority of parents who suffer significant mental ill health are able to care for and safeguard their children and/or unborn child but it is essential always to assess the implications for any children involved in the family.

5.3.2 Children most at risk of significant harm are those who feature within parental delusions and children who become targets for parental aggression or rejection, or who are neglected as a result of parental mental illness.

#### 5.3.3 The following parental risk factors may justify a referral to Children's Social Care for an assessment of the child's needs:

- Previous history of parental mental health especially if severe and / or enduring condition;
- Predisposition to, or severe post-natal illness;
- Delusional thinking involving the child;
- Self-harming behaviour and suicide attempts (including attempts that involve the child);
- Altered states of consciousness e.g. splitting / dissociation, misuse of drugs, alcohol, medication
- Obsessive compulsive behaviours involving the child;
- Non-compliance with treatment, reluctance or difficulty in engaging with necessary services, lack of insight into illness or impact on child;
- Disorder designated 'untreatable' either totally or within time scales compatible with the child's best interests;
- Mental illness combined with domestic violence and/or relationship difficulties;
- Unsupported and/or isolated mentally ill parents;
- Parental inability to anticipate needs of the child.

5.3.4 Care Programme Approach (CPA) assessments, Multi-Disciplinary meetings (MDT) or Professionals meetings about parents who have mental health difficulties, **must** include consideration of any needs or risk factors for the children concerned.

5.3.5 Psychiatrists should be involved in clinical decision making for services users who may pose a risk to children as above. This includes discharge planning and arrangements for home leave.

5.3.6 Where an adult, who is also a parent / carer, is deemed to be a danger to self or others a referral must be made to Children's Social Care. Children's Social Worker and Community Health Services e.g. Health Visitor, School Nurse, midwife must be invited to any relevant planning meetings and contribute toward a risk assessment if required.

### 5.4 Drug and Alcohol Misuse

5.4.1 As with mental illness in a parent, it is important not to generalise, or make assumptions about the impact on a child of parental drug and alcohol misuse.

5.4.2 Parental problem drug use can and does cause serious harm to children at every age from conception to adulthood. Parental misuse of drugs (prescribed and illegal) and/or alcohol is strongly associated with significant harm to children.

5.4.3 A Child Protection referral to Children's Social Care **must** always be made when:

- Combined domestic abuse and mental illness;
- The substance misuse of a parent or carer is chaotic or out of control;
- Drugs and paraphernalia (e.g. needles) are not kept safely out of reach of children;
- Children are passengers in a car whilst a drug or alcohol misusing carer is driving.

For all child protection referrals an incident form should also be raised via the Trust DATIX system and the referral form attached.

### 5.5 Domestic Abuse (*appendix 4*)

5.5.1 Domestic abuse refers to threatening behaviour, violence or abuse including, psychological, physical, sexual, financial or emotional. It also includes Female Genital Mutilation, Modern Day Slavery and Honour Based Violence.

5.5.2 Where there is evidence of domestic abuse, the implications for any children in the household must be considered and referral to Children's Social Care **must** be made where staff are aware of;

- A child's direct involvement with a domestic abuse incident or injury;
- A woman is pregnant. Pregnant women frequently experience punches and kicks directed at the abdomen, risking injury to both mother and foetus;
- Any child injured during episodes of violence or is witnessing the physical and emotional suffering of a parent.

5.5.3 The three objectives of any interventions when working with children and families where domestic abuse is a feature is:

- Protect the children
- Support the carer (non-abusive partner)
- Hold the abusive partner to account for their violence and offer opportunities for change

## 6.0 PROCEDURE: WHERE THERE ARE CONCERNS THAT A CHILD/REN HAS SUFFERED OR IS LIKELY TO SUFFER SIGNIFICANT HARM

6.1 If staff are concerned that a child or unborn baby has suffered or is likely to suffer significant harm then a referral to the relevant Children's Social Care Department must be made using the appropriate referral form for the area the family is living in. All referral forms are available via the Trust Intranet or via Local Authority

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

Staff should also raise an incident via DATIX and attach the appropriate referral form.

- 6.2 When there has been a serious injury or death of a child, staff are responsible for considering the welfare of other children in the household and reporting those concerns to their line manager, Safeguarding Team or Children's Social Care accordingly. All actions taken must be clearly recorded.
- 6.3 Where a child or parent discloses information to staff the staff member should record a clear and exact account of what was observed or said to them: In reference to child disclosures staff should.
  - Listen to the child rather than directly questioning further.
  - Never stop a child who is freely recalling significant events.
  - Write what was said verbatim, as well as time, setting and people present.
- 6.4 Staff should discuss any referral to Children's Social Care with the family unless this may:
  - Place a child at increased risk of significant harm e.g. by the behavioural response from parent/ carer
  - Place the staff member at risk;
  - Lead to the risk of loss of evidential material.
- 6.5 Reasons for not discussing the referral with the family should be recorded in case notes and within the referral.
- 6.6 Staff should not rely on a parent to pass on information about family difficulties to other professionals.
- 6.7 Referrals to Children's Social Care should be made within one day and may be made by telephone in some Local Safeguarding Partnership arrangement areas but must be followed up in writing within **48 hours** using the relevant referral form depending on the Local Authority area. Forms are accessible via the Trust Intranet Safeguarding page. The responsibility for undertaking section 47 enquiries lies with the local authority children's social care in whose area the child lives or is found, (location child suffers the incident of harm or neglect or identified to be at risk).
- 6.8 Whenever a referral is made staff should make clear exactly what the risks are or category of abuse. As much information as possible relating to the concern is required in order for Children's Social Care to make informed decisions regarding action to be taken. This includes an Early Help Assessment if used, relevant past medical/social history, staff involvement with family members, previous referrals, and views on parenting capacity. All decisions and actions taken must be recorded in the relevant child/ adult/family records.
- 6.9 Children's Social Care must acknowledge referrals within 1 working day of receipt of the written referral. Where no acknowledgement is received within 3 working days, the referrer must contact Children's Social Care again.
- 6.10 Where Children's Social Care decides to take no action, the referrer should anticipate feedback about that decision and its rationale. Where there is a disagreement or

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

concern regarding actions taken following a child protection referral then the Team Manager of the Social Care Team or the Trust Safeguarding Team should be contacted as per the local agreed escalation procedure.

- 6.11 Where there is a difference of opinion between Trust senior professionals regarding a risk to a child, the Named Nurse /Practitioner, Trust Safeguarding Team or the Service Director should be contacted.
- 6.12 If a referral needs to be made outside normal working hours then the Local Authority Emergency Duty Team or Police should be contacted Staff should contact the Manager on call via switchboard and record all discussions information and actions taken in the child/adults record..
- 6.13 Staff working with pregnant women should consider the need for a referral as soon as possible to Children's Social Care, so that assessments are undertaken and family support services can be provided as early as possible.
- 6.14 When a patient is admitted to an Adolescent Mental Health Inpatient Unit the admitting professional should contact Children's Social Care to check if a young person is known to them .Staff should use the *Yellow Internal Safeguarding Form* to record any safeguarding concerns that do not meet the threshold for a referral to social care and store in the young person's records.
- 6.15 If a young person does not have an allocated social worker the young person/ family should be offered a referral to social care for early help provision or as a child in need if required.
- 6.16 Where a young person has been referred to Children's Social Care, the Police and Social Care must be invited to all discharge planning meetings where appropriate.
- 6.16 Where a Looked After Child is admitted to an adolescent mental health inpatient unit the LAC Nurse and Social Worker must be informed and invited to all meetings including the discharge planning meeting. The admitting professional must request a copy of most recent LAC review including care plan from the allocated social worker.
- 6.17 Reports of suspected child abuse by a third party must be taken seriously and staff have a duty to advise the reporter to contact Children's Social Care directly. Staff cannot keep information confidential and have a responsibility to contact Social Care to ensure the concerns have been reported. All information and actions taken must be recorded in the child/adults records as appropriate.
- 6.18 Parental Responsibility**
- 6.18.1 Staff working in partnership with families should have knowledge of who holds parental responsibility as this will guide staff on how they share information and whose consent should be gained for actions taken on behalf of a child who is not old enough to have the capacity to make decisions.
- 6.18.2 Parental responsibility gives a parent the rights, duties, powers, responsibilities and authority of a child by law. A mother always has parental responsibility. A father has

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

parental responsibility if married to the mother at the time of birth or has acquired legal responsibility through

- Jointly registering the birth of a child with the mother (from Dec 1<sup>st</sup> 2003)
- By parental responsibility agreement with the mother
- By a parental responsibility order via a court.

The Family Court system can also grant parental responsibility in circumstances such as, emergency protection orders, adoption, or court orders etc. The Local Authority can acquire parental responsibility via a Care Order.

6.18.3 Staff working with children and young people must give due consideration to the child's wishes and feelings as far as is reasonably practicable giving due regard to the child's age and understanding. There will be occasions when it is not possible to ascertain the child's wishes and feelings. In these circumstances, professionals should record in writing the reasons.

### 6.19 Cross Boundary referrals

If a child lives outside the Trust area then the referral will need to be made to the relevant Local Authority where the child usually resides.

### 6.20 Assessment Framework

6.20.1 The *Framework for the Assessment of Children in Need and their Families (DoH 2000)* is a useful tool for staff to refer to when assessing children and families and completing reports for Case Conferences (see appendix 3) or Partnership meetings. The Framework contains three principle domains including;

- Child's development needs
- Parenting capacity to respond appropriately to those needs
- Wider family and emotional factors

ASSESSMENT FRAMEWORK TRIANGLE



6.20.2 Child's Development Needs

**Health**

Includes growth and development as well as physical and mental wellbeing. The impact of genetic factors and of any impairment needs to be considered. Involves receiving appropriate health care when ill, an adequate and nutritious diet, exercise, immunisations where appropriate and developmental checks, dental and optical care and, for older children, appropriate advice and information on issues that have an impact on health, including sex education and substance misuse.

**Education**

Covers all areas of a child's cognitive development which begins from birth. Includes opportunities: for play and interaction with other children to have access to books; to acquire a range of skills and interests; to experience success and achievement. Involves an adult interested in educational activities, progress and achievements, who takes account of the child's starting point and any special education needs.

**Emotional and Behavioural Development**

Concerns the appropriateness of response demonstrated in feelings and actions by a child, initially to parents and caregivers and, as the child grows older, to others beyond the family. Includes nature and quality of early attachments, characteristics of temperament, adaptation to change, response to stress and degree of appropriate self-control.

**Identity**

Concerns the child's growing sense of self as a separate and valued person. Includes the child's view of self and abilities, self-image and self-esteem, and having a positive sense of individuality. Race, religion, age, gender, sexuality and disability may all contribute to this. Feelings of belonging and acceptance by family, peer group and wider society, including other cultural groups.

### 6.20.3 Family and Social Relationships

Development of empathy and the capacity to place self in someone else's shoes. Includes a stable and affectionate relationship with parents or caregivers, good relationships with siblings, increasing importance of age appropriate friendships with peers and other significant persons in the child's life and response of family to these relationships.

### Social Presentation

Concerns child's growing understanding of the way in which appearance, behaviour, and any impairment are perceived by the outside world and the impression being created. Includes appropriateness of dress for age, gender, culture and religion; cleanliness and personal hygiene; and availability of advice from parents or caregivers about presentation in different settings.

### Self-Care Skills

Concerns the acquisition by a child of practical, emotional and communication competencies required for increasing independence. Includes early practical skills of dressing and feeding, opportunities to gain confidence and practical skills to undertake activities away from the family and independent living skills as older children. Includes encouragement to acquire social problem solving approaches. Special attention should be given to the impact of a child's impairment and other vulnerabilities, and on social circumstances affecting these in the development of self-care skills.

### 6.20.4 Parenting Capacity

#### Basic Care

Providing for the child's physical needs, and appropriate medical and dental care. *Includes* provision of food, drinks, warmth, shelter, clean and appropriate clothing and adequate personal hygiene.

#### Ensuring Safety

Ensuring the child is adequately protected from harm or danger. *Includes* protection from significant harm or danger and from contact with unsafe adults/other children and from self-harm. Recognition of hazards and danger both in the home and elsewhere.

#### Emotional Warmth

Ensuring the child's emotional needs are met giving the child a sense of being specially valued and a positive sense of own racial and cultural identity. *Includes* ensuring the child's requirements for secure, stable and affectionate relationships with significant adults, with appropriate sensitivity and responsiveness to the child's needs. Appropriate physical contact, comfort and cuddling sufficient to demonstrate warm regard, praise and encouragement.

#### Stimulation

Promoting child's learning and intellectual development through encouragement and cognitive stimulation and promoting social opportunities. *Includes* facilitating the child's cognitive development and potential through interaction, communication, talking and responding to the child's language and

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

questions, encouraging and joining the child's play, and promoting educational opportunities. Enabling the child to experience success and ensuring school attendance or equivalent opportunity. Facilitating child to meet to challenges of life.

### **Guidance and Boundaries**

Enabling the child to regulate its own emotions and behaviour. The key parental tasks are demonstrating and modelling appropriate behaviour and control of emotions and interactions with others, and guidance which involves setting boundaries, so that the child is able to develop an internal model of moral values and conscience, and social behaviour appropriate for the society within which they will grow up. The aim is to enable the child to grow into an autonomous adult, holding their own values, and able to demonstrate appropriate behaviour with others rather than having to be dependent on rules outside themselves. This includes not over protecting children from exploratory and learning experiences. *Includes* social problem solving, anger management, consideration for others, and effective discipline and shaping of behaviour.

### **Stability**

Providing a sufficiently stable family environment to enable a child to develop and maintain a secure attachment to the primary caregiver(s) in order to ensure optimal development. Includes: ensuring secure attachments are not disrupted, providing consistency of emotional warmth over time and responding in a similar manner to the same behaviour. Parental responses change and develop according to child's developmental progress. In addition, ensuring children keep in contact with important family members and significant others.

## **6.20.5 Family & Environmental Factors**

### **Family History and Functioning**

Family history includes both genetic and psychosocial factors.

Family functioning is influenced by who is living in the household and how they are related to the child; significant changes in family/household composition; history of childhood experiences of parents; chronology of significant life events and their meaning to family members; nature of family functioning, including sibling relationships and its impact on the child; parental strengths and difficulties, including those of an absent parent; the relationship between separated parents.

### **Wider Family**

Who are considered to be members of the wider family by the child and the parents? This includes related and non-related persons and absent wider family. What is their role and importance to the child and parents and precisely what way?

### **Housing**

Does the accommodation have basic amenities and facilities appropriate to the age and development of the child and other resident members? Is the housing accessible and suitable to the needs of disabled family members? Includes the interior and exterior of the accommodation and immediate surroundings. Basic amenities include water, heating, sanitation, cooking facilities, sleeping arrangements and cleanliness, hygiene and safety and their impact on the child's upbringing.

### **Employment**

Who is working in the household, their pattern of work and any changes? What impact does this have on the child? How is work or absence of work viewed by family members? How does it affect their relationship with the child? Includes children's experience of work and its impact on them.

### **Income**

Income available over a sustained period of time. Is the family in receipt of all its benefit entitlements? Sufficiency of income to meet the family's needs. The way resources available to the family are used. Are there financial difficulties which affect the child?

### **Family's Social Integration**

Exploration of the wider context of the local neighbourhood and community and its impact on the child and parents. Includes the degree of the family's integration or isolation, their peer groups, friendship and social networks and the importance attached to them.

### **Community Resources**

Describes all facilities and services in a neighbourhood, including universal services of primary health care, day care and schools, places of worship, transport, shops and leisure activities. Includes availability, accessibility and standard of resources and impact on the family, including disabled members.

## **7.0 RECORD KEEPING AND LIAISON**

- 7.1 The findings from a number of Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews have identified record keeping as a significant concern. The consequence of inadequate record keeping can result in confusion for professionals and may directly place a child or young person at risk.
- 7.2 All recordings regarding a child or adult constitute a legal document and can be used in court proceedings; therefore it is important to include all relevant information for all household members regardless of who the primary service user is.
- 7.3 All staff working directly with parents or carers should routinely record details of children in appropriate service user record e.g. Care Programme Approach (CPA) records, electronic records etc. Information must include the name, age and where the child is living. Additional information i.e. is the child registered with a GP and regularly attending school are important factors. Genograms must be used by all professionals where there are complex family structures or where this assists in identifying support needs or risks for the child. Genograms within CPA should be completed and updated regularly.
- 7.4 All records and assessments of parents and children must consistently record the racial, linguistic and religious identity and needs of the child and family
- 7.5 Staff should follow the Trust Record Keeping Policy. All discussions, decisions, actions and rationale for why no action is deemed necessary must be recorded contemporaneously with a date, name and signature. All recordings should be based on fact or professional opinion and kept in the service user's records.

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

7.6 At each new contact with a child or parent, the basic information about the child/ren should be checked and updated where applicable.

7.7 The records of service users who have children with a Child Protection Plan should indicate this clearly e.g. on significant event sheet or the appropriate local forms.

### 7.8 **Recording of relevant adult information by Community Health staff**

Community Health staff should use the relevant electronic/paper record to record information regarding parents/carers and significant others including.

- Relevant adult's individual care plans
- All appropriate medical information/reports.
- Relevant social details and background, place of residence, relationship to child.

7.9 Where available, relevant child /adult records and electronic service users systems should indicate or use an alert flag, that a child has a Child Protection Plan and include the category of abuse or neglect the child has suffered and the decisions in the plan relating to the member of staff's role. Additional alerts can be used to indicate domestic abuse, looked after children and exploitation within children's community records.

7.10 Relevant information from the child protection plan, Child in Need Plan /Partnership meeting relating to the parents/carers or significant others should be recorded in the adult records.

7.11 When a Child Protection Plan has been discontinued an entry in the Child Record/relevant adult record must indicate this.

7.12 It is important that all records, including the parent/carers adult records are kept together and if appropriate transferred together.

7.13 If part of the record has to be separated there must be an entry in the electronic/paper record stating where the retained record can be located.

### 7.14 **Personal Child Health Record (Red Book)**

- Normally contains all the findings and actions for the child from each visit.
- Should be used by all Community Health Professionals in contact with the child
- Will normally be completed with the parent /carer.

### 7.15 **Child Community Health Record (Health Visitors/School Nurses)**

- Contains all information relevant to the child e.g. chronology of significant event, domestic incident reports, case conference reports. (adult family member's information must be recorded in the appropriate record e.g. adult record).
- Records must indicate other Professionals involved including the GP

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

- Should reflect the needs assessment for the individual child.
- Include the discussions that have taken place with the family.
- Reflect points of discussion recorded in the parent held record.
- Child's views should be recorded.
- Observation of parent /child interaction or assessment of attachment should be recorded in the child's record
- A summary of assessment of need and outcome of the contact with a clear action plan should be made.

### 7.16 Use of body Maps

7.17 A Body Map must be completed whenever there are injuries or unusual findings including birthmarks, Mongolian Blue Spots and bruises or injury.

7.18 On the body map record:

- The child's details (Name, Dob, NHS no.)
- The size, shape, appearance and position of all unusual marks/ injuries
- An explanation as how the injuries were sustained.
- The behaviour and demeanour of both carer and child.
- Print staff name, designation and date.

7.19 Information that should be recorded includes:

- If the mark has been present from birth or early life
- Mark in suspicious area, around mouth or eyes, on ear which you think is a bruise
- Any bruise in a pre-mobile infant (under six months old)
- Infant with nose bleed, mouth bleed
- Skin blister in newborn/ infant
- Infant unwell or injured in any way
- Mongolian blue spots are purple, present in sacral area and satellite spots.
- No general welfare concerns + looks like a birth mark
- In most cases of inflicted 'precursor' bruise, parents usually concede mark is a bruise but the explanation suggests unreasonable force, e.g. held while feeding, or is implausible e.g. lying on dummy.

An entry should be made in the child's record referring to the body map.

### 7.20 Liaison

7.21 The Trust has liaison services and processes in place to support its Think Family approach. The process incorporates appropriate information sharing between Essex Accident and Emergency Departments, Essex Partnership University NHS Trust (EPUT) Mental Health Services and Essex Community Children's Service Providers regarding children and their parents/carers who attend hospital for emergency / unplanned care, the maternity unit or for babies admitted to Neo-natal Intensive Care.

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

- 7.22 When an Adult client is seen and assessed by the EPUT Assessment and Intervention or Crises teams in Essex A&E department's consideration will be given to whether there are safeguarding concerns where there is unborn – 18 year old child/children within the household.
- 7.23 The Assessment and Intervention or Crises team will discuss any identified concerns with the hospital's safeguarding team and where appropriate will make a safeguarding referral. When a safeguarding concern is identified a mental health notification form will be sent to the relevant community practitioner via the Paediatric Liaison Service. (EPUT Standards for Paediatric Liaison Service)
- 7.24 When there are concerns from the midwifery department or Primary Care for pregnant women an early ante natal referral liaison will take place with the relevant community children and where appropriate Perinatal Emotional Well Being team. Consideration should always be given as to whether a pre-birth assessment is indicated depending on the level of risk that is presented. Additionally if there are concerns from the in-patient midwifery team regarding additional care needs during the immediate post-natal period not previously identified it is expected that a liaison notification will be made to the relevant adult mental health or Children's Community Services practitioners involved in the clients care from the midwifery team.

### **8.0 ACCESS TO INFORMATION**

- 8.1 All Trust staff have a duty to assist Social Care with Section 47 enquiries when a child is believed to be suffering or at risk of suffering significant harm.
- 8.2 If a member of staff is approached via telephone for information on a child by a Social Worker or other professional, the member of staff must identify whom they are speaking to and if they do not recognise the caller phone back.
- 8.3 Record details of caller and time and the action taken in the Child and relevant Adult Record.
- 8.4 Safe sharing of information principles must be applied including:
- Ensuring information is to a secure email address or the document is password protected which is sent separately.
  - Child/family details should not be emailed to any other agency outside of health unless a secure system is used in accordance to the Trust security policy.
  - Posted information should be marked private and confidential and include a compliment slip from sender.
- 8.5 If any other person, including parents/carers, request information about a child, parent or third party staff should contact the line manager or the Safeguarding Children Team for advice.
- 8.6 Health records will not normally be released to persons outside the Health Service except on Court Orders. However parents have a right of access to their child's records. If a request is made for access, contact the Line Manager in the first instance. Further advice can be sought from the Named Nurse Safeguarding Children or Trust Information Governance Manager or Trust Legal

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

Representative. Further guidance can be found within the Trust 'access to records' policy.

### 8.7 Formal statements & Court Process

- 8.7.1 Staff are required to co-operate with police and the Local Authority when approached for a formal statement.
- 8.7.2 In these circumstances staff must inform the relevant Safeguarding Team and their line manager. The Trust Legal Advisor can be contacted for advice and support. Appendix 11 gives additional guidance for those staff giving formal statements or attending court as a witness

## 9.0 MISSED APPOINTMENTS, NON COMPLIANCE & HOSTILE CARERS

- 9.1 Parents/Carers failure to attend health appointments for a child/ren has been a feature of a number of Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews and staff working with children should note all missed appointments and consider any safeguarding concerns. It is the weight and significance placed on missed appointments, in conjunction with their frequency and cumulative impact on the health of children which may constitute neglect by their parents, who either by omission or commission fails to safeguard their children's health by not attending a recommended contact with health services.
- 9.2 Missed appointments to health services should be notified to the referrer, the GP and relevant health professional (Health Visitor or School Nurse etc.). Staff should also consider if patterns of missed appointments has been seen in other children in the family.
- 9.3 Where there are failed telephone contacts with other professionals or parents/carers regarding a child then staff should formalise this in writing requesting contact and stating how this can be achieved. If there continues to be no response then staff should escalate this to the named Social Worker (if child has one) and the Safeguarding Team. The GP should be notified where appropriate. All attempts at contact should be fully documented in the health record.
- 9.4 Staff working with parents who fail to attend health appointments should consider the impact this may have on the parenting capacity of children or for pregnant women, the impact on the unborn. Mental health staff or those working in Community Drug & Alcohol or Adult Learning Disability Teams should consider discussing missed appointments with the relevant health visitor, school nurse or midwife in order to share information and assess levels of concern and risk.
- 9.5 Parents should be notified when failing to attend appointments and offered an alternative appointment or discussion on any assistance required in order to facilitate attendance. If staff are concerned regarding the impact of failing to attend appointments for an adult or child on a child's welfare they should:
- Discuss with their line manager or manager of service
  - Discuss with a member of the Safeguarding Team
  - Consider a partnership meeting

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

- Consider a referral to children's social care
- Add this information to the Chronology of significant events

### 9.6 Hostile or non-compliant parent/carers

9.7 Staff should ensure that the needs of the child in a family are paramount regardless of who the primary service user is.

9.8 Hostile parents refer to those who are or have been violent, aggressive, threatening or intimidating in a physically, verbally or emotionally damaging way. This may be directed at staff, partners, children or animals. In these circumstances staff must consider the safety of any child/ren in the home and discuss with the parents key worker if a Trust service user, line manager or the Named Safeguarding Nurse/Practitioner.

### 9.9 Non compliance

This includes a wide range of deliberate behaviours and attitudes intended to restrict the effectiveness of any intervention in place to safeguard the child/ren e.g. child protection plan. It can include actively undermining efforts to bring about change or passively not complying with plans or disguised compliance whereby parents do not admit to their lack of commitment to change but work subversively to undermine the process.

9.10 Staff working with the adult parent or child should be mindful of underlying reasons for non-compliance or lack of co-operation. Factors associated with hostility and non-compliance include Domestic Abuse, Fear of statutory services, Isolation, Immigration status etc.

9.11 It is important that staff should consider the impact of non-compliance on the child/rens welfare and safety and all identified risks should be shared with both health and multi-agency colleagues working with a particular family. This includes Children's Social Worker GP, Psychiatrist etc. Workers must recognise when the family is not engaging so as to avoid collusion or avoidance. Early recognition of family resistance is critical.

9.12 The line manager and the Named Nurse/Practitioner Safeguarding should be informed and staff should give regard to the Trust Lone Working Policy RM17.

9.13 Community Health staff making home visits where there are child protection concerns must see the child. Any risk assessment should be recorded in the child's health records. Where staff are not entirely satisfied with compliance, the clinical, social or emotional picture that is presented or where maltreatment is suspected they should consider a child protection referral to Children's Social Care

## 10.0 HISTORICAL ABUSE ALLEGATION

10.1 Adult or child service users who disclose they have been abused in the past e.g. sexual abuse or female genital mutilation must be treated sensitively. Service users should be offered information, support or counselling etc.

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

10.2 Police must be informed about allegations of a crime at the earliest opportunity. Whether they become involved in an investigation will depend on several factors including the victim's wishes and public interest. Staff may discuss this with the Police Child Abuse Investigation Unit or the Trust Safeguarding Team.

### 11.0 VULNERABILITY, COMPLEX FACTORS & ADDITIONAL NEEDS

11.1 Staff working with children or adults must consider the support needs required to maintain a child's welfare in all aspects of their work. This should be routinely considered within the Care Programme Approach (CPA), Community Health Service and Adolescent Mental Health or Children's Learning Disability assessments and revisited at each contact with a parent or child.

11.2 When working in either adult or child settings, staff should be aware that a number of Vulnerability Factors will affect children's welfare such as; Social Exclusion, Bullying, Missing Children/Families, Forced Marriages, Honour Based Violence, Migrant Children, Disabled Children, Child Sexual Exploitation and Female Genital Mutilation, Modern day slavery and those at risk of violent extremism or radicalisation etc.

#### 11.3 Community Based Violence

Significant harm and additional vulnerability factors can apply to young people, from community based violence such as gang, group and knife crime. In these circumstances staff need to ensure that the safeguarding process responds effectively to involve both the perpetrators and victims of violent activity.

11.3.1 Exposure to, or involvement with, groups or individuals who condone violence as a means to a political end is a particular risk for some children. Children and young people can be drawn into violence themselves or they can be exposed to messages through direct contact with members or, increasingly, through the internet. This can put a young person at risk of being drawn in to criminal activity or recruited by violent extremists.

#### 11.4 Prevent

11.4.1 CONTEST is the Government's national counter terrorism strategy, aims to reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence.

The strategy has four work streams:

Pursue: to stop terrorist attacks

Protect: to strengthen our protection against terrorist attack

Prepare: where an attack cannot be stopped, to mitigate its impact

**Prevent: to stop people becoming terrorists or supporting terrorism**

11.4.2 **Prevent** aims to stop people from becoming terrorists or supporting terrorism. The Trust guidance on Prevent (appendix 12) reflects the Home Office Strategy *Building Partnerships Staying Safe*.

The Prevent Strategy addresses all forms of terrorism including extreme right wing but continues to prioritise according to the threat posed to our national security. The

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

aim of Prevent is to stop people from becoming terrorists or supporting terrorism and operates in the pre-criminal space before any criminal activity has taken place.

The Trust Prevent protocol reflects the Home Office policy May 2015. Staff concerned that a child or family may be affected by violent extremism must consult their line manager, or a member of the Safeguarding Team.

### 12.0 EARLY HELP ASSESSMENT (EHA)

12.1 All staff are required to identify emerging problems and potential unmet needs for individual children and families and to share information with other professionals to support early identification and assessment. Professionals should be alert to the potential need for early help for a child who:

- Is disabled and has specific additional needs
- Has Special Educational Needs (SEND) whether or not they have a statutory Education, Health Care Plan (EHCP)
- Is a young carer
- Is showing signs of being drawn into anti-social or criminal behaviour, including gang involvement and association with organised criminal groups
- Is frequently missing/goes missing from care or from home
- Is at risk of modern slavery, trafficking or exploitation
- Is at risk of being radicalised or exploited
- Is in a family circumstance presenting challenges for the child such as substance misuse, adult mental health problems or domestic abuse
- Is misusing drugs or alcohol themselves
- Has returned home to their family from care
- Is showing early signs of abuse or neglect.

12.2 The Early Help Assessment (EHA) is a holistic and generic assessment of a child or young person's needs for additional services. It is a helpful tool for staff working in partnership with parents to identify extra support when there is a concern about how well a child (or unborn baby) or young person is progressing, when their needs are unclear, or broader than Trust services can address on its own. A common assessment would help identify the needs, and provide a basis for getting other services involved. Providing early help is more effective in promoting the welfare of children than reacting later. Early help means providing support as soon as a problem emerges, at any point in a child's life, from the foundation years through to the teenage years.

12.3 Effective early help relies upon local agencies working together to:

- Identify children and families who would benefit from early help;
- Undertake an assessment of the need for early help; and
- Provide targeted early help services to address the assessed needs of a child and their family which focuses on activity to significantly improve the outcomes for the child. Local authorities, under section 10 of the Children Act 2004, have a responsibility to promote inter-agency cooperation to improve the welfare of children.

12.4 Children and families may need support from a wide range of local agencies. Where a child and family would benefit from coordinated support from more than one agency

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

(e.g. education, health, housing, police) there should be an inter-agency assessment. These early help assessments should identify what help the child and family require preventing needs escalating to a point where intervention would be needed via a statutory assessment under the Children Act 1989.

- 12.5. The early help assessment should be undertaken by a lead professional who should provide support to the child and family, act as an advocate on their behalf and coordinate the delivery of support services. The lead professional role could be undertaken by a General Practitioner (GP), family support worker, teacher, health visitor and/or special educational needs coordinator. Decisions about who should be the lead professional should be taken on a case by case basis and should be informed by the child and their family.
- 12.6 The EHA process must be undertaken in partnership with parents and children and the principles will also be incorporated into the Trust Care Programme Approach (CPA) Handbook, and the Trust Safeguarding Intranet Link.
- 12.7 All Local Safeguarding Partnership areas within the Trust will use their own Early Help Assessment form so staff should refer to the Trust safeguarding or Local Safeguarding Partnership arrangements intranet sites for their local forms.
- 12.8 If parents and/or the child do not consent to an early help assessment, then the lead professional should make a judgement as to whether, without help, the needs of the child are likely to escalate and place the child at risk of significant harm. If it is felt that this is so, a referral into local authority children's social care may be necessary.

### 13.0 IMPLEMENTATION

- 13.1 Copies of these procedural guidelines and the associated policy is available on the Trust Intranet,
- 13.2 Staff awareness of these procedural guidelines will be raised via Trust communications and all Trust Safeguarding and Clinical Governance Groups. Policy Holders are responsible for ensuring all staff in their areas are aware of any updates
- 13.3 In implementing these procedural guidelines all staff should:
  - Be aware of the legal framework when dealing with children;
  - Ensure minimal delay in resolving matters;
  - Ensure that all children are treated with equal respect regardless of race, gender, religion, sexual identity or impairment.

**14.0 MONITORING & REVIEW**

- 14.1 The Trust Safeguarding Team will ensure an audit of key parts of this policy will be undertaken every three years with a rotating theme for example; recommendations from Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews, the referral process to Social Care, support offered to staff, duties being undertaken appropriately and training uptake.
- 14.2 The Safeguarding Team will provide advice on the review and appropriate changes to this procedure following lessons learnt from incidents both nationally and locally.

**END**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

TRAINING FRAMEWORK FOR SAFEGUARDING CHILDREN & ADULTS

1.0 INTRODUCTION

1.1 All Health Trusts have a statutory duty to ensure every member of staff is competent and confident in carrying out their Safeguarding responsibilities appropriate to their role and remit. This Framework applies to Children and Adults has been informed by the following documents:

1.2 **Children**

Safeguarding Children and Young People Roles and Competencies for Health Care Staff 2019.  
Intercollegiate Framework for Looked After Children (2015).  
DoH Working Together to Safeguard Children 2018.  
National Service Framework (Standard 5).  
Local Safeguarding Children Board Procedures.  
Building Partnerships, Staying Safe 2011.

1.3 **Adults**

The Care Act 2014.  
Adult Safeguarding Roles and Competencies for Health Care Staff 2018  
Local Safeguarding Adult Boards Competency Framework and Training Strategy for Safeguarding Adults.  
Mental Capacity Act and Deprivation of Liberty Safeguards 2015.  
Building Partnerships, Staying Safe 2011.

1.4 This Framework introduces a training levels underpinned by Agenda for Change Knowledge and Skills framework (KSF) Core Dimension 3 which focuses on maintaining and promoting health safety and security of all those who come into contact with Trust services. In addition, Specific Dimension HWB3 Protection of Health and Well Being which focuses on protecting people when there are risks.

2.0 PURPOSE

2.1 All Trust staff, including non-clinical staff **must** consider the welfare of Children and Adults irrespective of whether they are primarily working with adults or with children and young people.

2.2 This Framework affords staff the opportunity to understand and have the necessary knowledge, skills, attitudes and values to carry out their responsibilities and be aware of safe practice within their work setting with regard to Safeguarding Children and Adults including Looked After Children (LAC) Prevent, Mental Capacity and Deprivation of Liberty Safeguards (MCA DoLS).

- 2.3 This Framework provides a training programme which meets individual training requirements in accordance with specific competency needs within EPUT.
- 2.4 The Framework makes optimal use of the Local Safeguarding Partnership arrangements multi-agency training programmes to promote partnership working.
- 2.5 This Framework ensures that a programme of in house training is in place for all staff including Doctors that supports the delivery of national and local developments. Locum staff should have either undertaken Safeguarding training or have access to in house training.

### **3.0 QUALITY ASSURANCE**

- 3.1 The Trust has a responsibility to ensure that all Safeguarding training (including LAC and Prevent training) is delivered to a consistently high standard, and that a process exists for evaluation of training effectiveness. This responsibility includes ensuring that:
- 3.2 Training is delivered by trainers who are knowledgeable about processes for Safeguarding Children and Adult and have facilitation skills.
- 3.3 Training reflects understanding of the rights of children and adults and is informed by an active respect for diversity and a commitment to ensuring equality of opportunity:
- Training is informed by current research evidence, lessons from Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews, local and national developments and initiatives
  - All training includes a statement of the learning outcomes specific to the appropriate level.
  - The Safeguarding Children and Adult annual reports for the Trust Board will include a report on training and be available via the Trust Intranet Safeguarding site.

### **4.0 PROCESS**

- 4.1 The Trust Safeguarding Training Framework and the Mandatory Training Procedure HPG21 outlines the requirement that **all** EPUT staff must receive Safeguarding Adult and Children Training every three years as *per Table 1*. New staff must access level 1 & level 2 OLM training as appropriate to their role during their induction period within three months of start date. Specific staff are also required to access Looked After Children (LAC) training, Prevent training and MCA & DoLS training.
- 4.2 There are a number of different levels of training dependant on Trust staff role, specialism and contact with adults or children.

## CLPG37 - SAFEGUARDING CHILDREN PROCEDURE

### APPENDIX 1

- 4.3 All staff should receive an update on safeguarding annually. This does not require attendance at formal training sessions but can be via a team discussion, case study, newsletter, shadowing a colleague etc. The Trust Intranet Safeguarding page contains regular updates for team discussion.
- 4.4 Training can be accessed via the Trust Oracle Learning Management (OLM), Local Safeguarding Partnership arrangements, and National Conferences etc. Training content should comply with the Competencies set out within the Intercollegiate Document 2019 and these Competencies should be reviewed annually as part of staff appraisal system.
- 4.5 The Workforce Development and Training Department will report monthly on compliance levels to the Trust Executive Team and the Trust Mental Health Act and Safeguarding Sub-Committee. Compliance for all training is set at 95% of the true total of staff.
- 4.6 Monthly mapping reports will also be sent to operational managers and directors identifying which of their staff are up-to-date and when they are approaching update deadlines. Non-attendance of courses will also be recorded.
- 4.7 Regular mapping of roles and subsequent training level takes place therefore the list below can change in accordance with newly developed roles or the acquisition of different services. The Trust Safeguarding team work closely with the Workforce development team to ensure effective systems are in place to notify and monitor training.

## 5.0 SAFEGUARDING TRAINING

### 5.1 Levels of Training include:

- Level 1      Safeguarding Children & Adults**  
ALL Non clinical staff (with no contact with children or adults)
- Level 2      Safeguarding Children & Adults**  
Incorporates Level 1-All Clinical Staff including Doctors and those non clinical staff who have contact with children or adults.
- Level 3      Safeguarding Children Training**  
*‘All clinical staff working predominantly with children, young people and parents who contribute toward assessing, planning and evaluating the needs of children and parenting capacity where there are safeguarding concerns’ (Intercollegiate Document March 2019)*
- Level 4      Specialist Safeguarding Children training**  
Named and Designated Safeguarding Team staff

**The staff above will be prioritised when applying for a place. If staff other than those above wish to attend Level 3 and they have their**

manager's agreement then they can apply and will be given a place if available.

## **6.0 LOOKED AFTER CHILDREN (LAC) TRAINING**

There are three levels of LAC training. Level 1 and 2 are integrated into safeguarding training Level 1&2 as demonstrated in the tables in Section 12 below.

### **6.1 Level 3 LAC Awareness- OLM**

Staff working directly with Looked After Children will require awareness training for Looked after Children which is relevant to their role e.g. clinical staff who contribute regularly to address the health needs of a looked after child. The training is competency based and is mapped against the Intercollegiate Framework for Looked After Children (2015).

### **6.2 Level 3 LAC Health Assessment Training, Face to Face – full day**

Looked After Children health assessment training is specialist training for all clinical staff who undertake statutory health review assessments for looked after children. Staff must have completed Level 3 OLM.

## **7.0 PREVENT TRAINING**

7.1 All Trust staff are expected to access basic awareness training in Prevent and this is incorporated into Safeguarding Level 1-3 Safeguarding training as outlined in section 12.

7.2 Specific staff (Sec 12 table 6) are also required to access PREVENT Health Workshop to Raise Awareness of Prevent (WRAP). These staff must complete the OLM package and does not need to be repeated.

## **8.0 ACCESS TO TRAINING**

8.1 The Trust Safeguarding Team in conjunction with the Workforce Development & Training Department and Trust Training Bulletin will circulate details of all available training for staff.

8.2 Safeguarding training is mandatory and all staff will be able to use their training tracker to identify which level of training is appropriate for them. Staff must follow Trust processes to access training via the Mandatory Training Guidance HRP21.

Staff who would like to access training not on their tracker as a mandatory requirement are welcome to attend any course (where spaces are available) and should discuss with their manager and contact the training dept. accordingly.

Training available from other organisations may require staff to complete an additional application form but it is **vital** that the Trust form is also completed in order that staff are registered on the Trust data system as having received training.

- 8.3 The Safeguarding professionals can be contacted by staff to discuss individual safeguarding training requirements.
- 8.4 Staff can access further information on training from their geographical LSCB websites.
- 8.5 Additional supplementary Safeguarding training will be considered in line with Local Safeguarding Partnership arrangements Learning and Improvement strategies. These will include learning from Local Child Safeguarding Practice Reviews formally known as Serious Case Reviews (national & local) and any changes in legislation/statutory guidance and local audit/case reviews.
- 8.6 Operational line managers and individual staff should consider supplementary safeguarding training as part of Personal Development Programme.

## **9.0 AUDIT & EVALUATION**

- 9.1 Training programs will be regularly evaluated to ensure that they meet the agreed learning outcomes.
- 9.2 Audits of Trust training will contribute towards the Local Safeguarding Partnership arrangements training reports.
- 9.3 Trust staff may be contacted and expected to inform safeguarding training evaluation processes, following participation in training events.

## **10.0 MONITORING & DATA COLLECTION**

- 10.1 The Workforce, Training and Development department maintain data on
  - those applying for and attending training.
  - the numbers from particular staff groups that attend training.
- 10.2 The Safeguarding Team maintains data on all training they have delivered and send attendance lists to the Training Department.

## **11.0 REPORTING ARRANGEMENTS**

- 11.1 Performance reports are presented internally and externally from the Trust.
- 11.2 A performance report will be included in all Safeguarding annual reports.
- 11.3 Training reports will be shared with the Local Safeguarding Partnership arrangements where required.

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

11.4 The Training Framework will be agreed by the Safeguarding team and Workforce Planning Group before being approved by the Mental Health Act & Safeguarding Sub-Committee.

**12.0 TRAINING REQUIREMENTS**

The following table outlines the Training requirements for Trust Clinical and Non Clinical Staff

**12.1 TABLE 1**

**LEVEL 1: SAFEGUARDING CHILDREN & ADULTS**

<b>STAFF REQUIREMENTS</b>	<b>ALL NON CLINICAL STAFF</b>
<b>METHOD</b>  Updates	<b>OLM / E-LEARNING</b>  A written update or briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news team meetings etc.
<b>FREQUENCY</b>  <b>DURATION</b>	<b>Repeat every three years</b>  <b>Minimum 2 hours</b>
Competency	<ul style="list-style-type: none"> <li>• Understand what constitutes child/adult abuse.</li> <li>• Know the range of categories of abuse.</li> <li>• Know what to do when there are concerns that a child or adult is being or is at risk of suffering significant harm.</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>• Know about local policies / procedures.</li> <li>• Know who to contact if staff have concerns.</li> <li>• Understand the importance of sharing information, how it can help and the dangers of not sharing information.</li> <li>• Know what the term Looked After Child (LAC) means</li> <li>• Awareness of the role of the Local Safeguarding Partnerships</li> <li>• Honour Based Abuse e.g. Female Genital Mutilation</li> <li>• Prevent</li> <li>• Child Sexual Exploitation and Exploitation</li> <li>• Modern day slavery and Child Trafficking</li> <li>• MCA DOLS</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• Be able to recognise signs of child /adult abuse as this relates to their role.</li> <li>• Be able to seek advice and report concerns, ensuring that they are listened to.</li> </ul>
Attitudes & Values	<ul style="list-style-type: none"> <li>• Willingness to listen to children &amp; young people and act on concerns.</li> </ul>

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

**12.2 TABLE 2**

**LEVEL 2: (Incorporates level 1) SAFEGUARDING CHILDREN & ADULTS**

<b>STAFF REQUIREMENTS</b>	<b>ALL CLINICAL STAFF</b>
<b>METHOD</b>  Updates	<b>OLM / E-LEARNING</b>  A written update or briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news team meetings etc.
<b>FREQUENCY</b>	Staff should repeat this training every three years if they only complete one of the level 3 safeguarding training i.e. either adults or children training packages. No update is required if staff have completed both level 3 safeguarding children and adult training packages.
<b>DURATION</b>	<b>Minimum of 4 hours</b>
Competency	<ul style="list-style-type: none"> <li>• As level 1.</li> <li>• Be able to recognise child /adult abuse.</li> <li>• Be able to document concerns.</li> <li>• Know who to inform.</li> <li>• Understand the next steps in the child/adult safeguarding process.</li> <li>• Be aware of relevant legislation</li> <li>• Be able to identify and refer for concerns of Prevent, Honour Based Abuse e.g Female Genital Mutilation in addition to Child Sexual Exploitation, Exploitation and MCA DoLS</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>• As level 1.</li> <li>• Understand risk factors associated with Safeguarding i.e. domestic abuse, drug/alcohol misuse, parental mental health concerns</li> <li>• Understand the needs of the child are paramount</li> <li>• Understand the need for Capacity Assessments for safeguarding adults</li> <li>• Understand Deprivation of Liberty Safeguards</li> <li>• Understands the purpose and need for Child Practice Reviews</li> <li>• Understand the increased needs on Looked After Children</li> <li>• Awareness of Local Safeguarding Partnerships</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• As level 1.</li> <li>• Be able to document child/adult concerns, differentiating between fact and opinion.</li> <li>• Where further support is needed, know when to take action and when to refer to managers or the Safeguarding Team.</li> </ul>
Criteria for assessment	<ul style="list-style-type: none"> <li>• As level 1.</li> <li>• Demonstrates appropriate referral for assessment for family support to reduce risks of child /adult maltreatment.</li> <li>• Demonstrates the referral process using the appropriate referral forms for Safeguarding concerns</li> <li>• Demonstrates accurate documentation of concerns.</li> </ul>
Attitudes & Values	<ul style="list-style-type: none"> <li>• Recognises how own beliefs, experience and attitudes might influence professional involvement in safeguarding work</li> </ul>

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

**12.3 TABLE 3**

**LEVEL 3:**

**SAFEGUARDING CHILDREN TRAINING**

<p><b>STAFF REQUIREMENTS</b></p>	<p>Health Visitors, School Nurses, Community staff nurses 0-19 team service, Locality Leads for Children (Bedford), Locality Managers for Children, Heads of service for Children's Community Services, Team leaders in Children's Community Services, Modern Matrons for Children's Community Services, Family Nurse Practitioners, Paediatric Nurses and Doctors, Registered Paediatrics allied health professionals, CAMHS Registered staff and doctors, Consultant Psychiatrists, Learning Disability Nurse Team Manager/ Heads of Service, Community Drug &amp; Alcohol registered staff (STaRS), Community Psychiatric Nurses Band 5-7, Community Social Workers, Safeguarding Practitioners, Sexual Health staff. e.g. senior nurses for CASH, Clinical Nurse Specialists for CASH, modern matrons for CASH, Chlamydia screening coordinator and Nurse practitioner for Chlamydia. Lead Immunisation Nurses and Lead Nursery Nurses</p> <p>(Staff working in Older Peoples services are <b>NOT</b> required to attend however; if any staff other than those above wishes to attend Level 3 and they have their manager's agreement then they can apply and will be given a place if available.</p>
<p><b>METHOD</b></p> <p>Updates</p>	<p><b>Face to Face</b></p> <p><b>A written update or briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news, team meetings etc.</b></p>
<p><b>FREQUENCY</b></p> <p><b>DURATION</b></p>	<p><b>Repeat every three years</b></p> <p><b>Minimum 8 hours</b></p>
<p>Competency</p>	<ul style="list-style-type: none"> <li>• As level 2.</li> <li>• Knowledge of the implications of key national document / reports.</li> <li>• Understand the assessment of risk and harm.</li> <li>• Understand multiagency framework and Information sharing</li> <li>• Be able to present Safeguarding Children concerns in a Safeguarding conference or meeting.</li> <li>• Puts into practice knowledge of how to reduce risks of harm.</li> <li>• Ability to contribute to child practice reviews or serious case reviews for children or adults.</li> <li>• Prevent, FGM, Exploitation, CSE, Gangs, Cuckooing and Honour based abuse</li> </ul>
<p>Knowledge</p>	<ul style="list-style-type: none"> <li>• As level 2.</li> <li>• Aware of implications of recent legislation / national documents.</li> <li>• Understand multi-agency frameworks on assessment processes, including the use of the Common Assessment Framework.</li> <li>• Understand the basics of forensic procedures.</li> <li>• Some understanding of Fabricated or induced illness(FII)</li> <li>• Aware of resources that may be available within health and other agencies, including the voluntary sector, to support adult's children or families in need.(Advocates, Independent Mental Capacity Advocate IMCA)</li> </ul>

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

	<ul style="list-style-type: none"> <li>• Know what to do when there is an insufficient response from other organisations or agencies.</li> <li>• Understand the process for following up failure to attend appointments</li> <li>• Awareness of the function of the Local Safeguarding Partnerships</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• As level 2.</li> <li>• Be able to undertake an assessment of risk.</li> <li>• Be able to identify and outline the management of children in need.</li> <li>• Be able to instigate measures to reduce the risk of abuse occurring.</li> </ul>
Attitudes & Values	<ul style="list-style-type: none"> <li>• Understands the impact of a family's cultural /religious background when assessing risks</li> <li>• Understand the potential personal impact of safeguarding work on staff and the need for effective support and supervision</li> </ul>
Criteria for assessment	<ul style="list-style-type: none"> <li>• As level 2.</li> <li>• Demonstrates advanced knowledge of patterns and indicators of maltreatment.</li> <li>• Demonstrates understanding of information sharing issues related to child protection, children in need and adult protection.</li> <li>• Demonstrates knowledge of each agency's role and responsibilities within local policies and procedures.</li> </ul>

**12.4 TABLE 4**

**LEVEL 4-6**

**SPECIALIST SAFEGUARDING TRAINING**

<b>STAFF REQUIREMENTS</b>	Named Safeguarding Team members
<b>METHOD</b>  Updates	<b>Face to Face</b>  <b>A written update or briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news, team meetings etc.</b>
<b>FREQUENCY</b>  <b>DURATION</b>	<b>Repeat every three years</b>  <b>24 hours within three years</b>
Competency	As per Level 1-3 and <ul style="list-style-type: none"> <li>• Able to implement and audit the effectiveness of Safeguarding services on an organisational level.</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>• Understand the Commissioning and planning of safeguarding services</li> <li>• Advanced understanding of Information Governance</li> <li>• Know about the Experts role in the Court process.</li> </ul>
	As Level 1-3

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

Skills	<ul style="list-style-type: none"> <li>• Able to give advice on policy and legislative Frameworks.</li> <li>• Able to advise other agencies on health management and services related to Safeguarding.</li> <li>• Able to participate in Child Practice Reviews, Serious Case Reviews, Homicide Reviews and IMR's.</li> <li>• Able to lead service reviews.</li> <li>• Able to establish Quality assurance measures and processes.</li> <li>• Able to deal with media and organisational public relations concerning Safeguarding and the impact on the Trust.</li> </ul>
Criteria for assessment	<ul style="list-style-type: none"> <li>• Demonstrates a knowledge of the process of Child Practice, SCR and Homicide Reviews.</li> <li>• Demonstrates knowledge of performance indicators, trends and analysis of Safeguarding data and the implications for Trust clients and services.</li> <li>• Demonstrates knowledge of functions of Local Safeguarding Partnerships.</li> </ul>

**12.5 TABLE 5:**

**LEVEL 3**

**LOOKED AFTER CHILDREN TRAINING**

<b>STAFF REQUIREMENTS:</b>	<b>Staff working in Community Health Services and CAMHS working directly with Looked After Children (as per list 12.3. Safeguarding Children Level 3)</b>
<b>METHOD</b>  Update	<b>OLM E-Learning or direct face to face session</b>  <b>A written update or briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news team meetings etc.</b>
<b>FREQUENCY</b>  <b>DURATION</b>	Every three years  <b><u>LAC Awareness: via OLM</u></b> This course encompasses a full day for those clinical staff who contribute regularly to address the health needs of a Looked After Child.  <b><u>LAC RHA: Full Day Face to face</u></b>  Targeted Looked After Children health assessment training All clinical staff who undertake statutory health review assessments for looked after children.
Competency	<ul style="list-style-type: none"> <li>• Knowledge of the implications of key national document / reports.</li> <li>• Understand the assessment of risk and harm.</li> <li>• Understand multiagency framework and Information sharing.</li> <li>• Ability to contribute to serious case reviews for children or adults.</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>• Understands the impact of ante-natal factors and adverse life events on a child's development, physical health, emotional wellbeing,</li> <li>• Knows the increased vulnerability of this group to substance misuse,</li> </ul>

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

	<p>self-harm, sexual exploitation, criminality, teenage pregnancy, and exclusion from education, mental, emotional and behavioural difficulties.</p> <ul style="list-style-type: none"> <li>• Understands issues around consent, confidentiality and the implications of data protection relevant to their own role.</li> <li>• Understands own role within the multi-agency framework, assessment, care planning and monitoring.</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• Able to contribute to the statutory health assessment and implementation of health care plans, and when requested contribute via report or attendance at Statutory LAC Review.</li> <li>• Able to identify and advise local authorities in respect of special educational needs.</li> <li>• Able to build positive relationships with parents/carers and be skilled in managing conflict and difficult behaviours.</li> <li>• Able to identify the need for further specialist support, advice, and supervision in situations where the looked after child's problems require further expertise or intervention such as in relation to sexual health, emotional or mental health, developmental difficulties and/or the disabled children and take appropriate action.</li> </ul>
Attitudes & Values	<ul style="list-style-type: none"> <li>• Understands the impact of a family's cultural /religious background when assessing risks</li> </ul>

**TABLE 6**                      **PREVENT: Working to Raise Awareness of Prevent (WRAP)** *(Please note: basic Prevent training is incorporated within Level 1-3 Safeguarding courses for ALL Trust staff. Below is specialised Prevent training programme))*

<b>STAFF REQUIREMENTS</b>	<p>Health Visitors, School Nurses, Community staff nurses 0-19 team service, Locality Leads for Children (Bedford), Locality Managers for Children, Heads of service for Children's Community Services, Team leaders in Children's Community Services, Modern Matrons for Children's Community Services, Family Nurse Practitioners, Paediatric Nurses and Doctors, Registered Paediatrics allied health professionals, CAMHS Registered staff and doctors, Consultant Psychiatrists, Learning Disability Nurse Team Manager/ Heads of Service, Community Drug &amp; Alcohol registered staff, Community Psychiatric Nurses Band 5-7, Community Social Workers, Safeguarding Practitioners, Sexual Health staff. e.g. senior nurses for CASH, Clinical Nurse Specialists for CASH, modern matrons for CASH, Chlamydia screening coordinator and Nurse practitioner for Chlamydia. Lead Immunisation Nurses and Lead Nursery Nurses.</p>
<b>METHOD</b>  Update	<p><b>OLM E-LEARNING</b></p> <p><b>A written update briefing of any changes in legislation and practice from the Trust Safeguarding Team will be available at a minimum of annually via Trust news team meetings etc.</b></p>

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 1**

<b>FREQUENCY DURATION</b>	<b>ONCE ONLY</b>  <b>1- 1.5 hours</b>
Competency	<ul style="list-style-type: none"> <li>• Knowledge of the implications of key national document / reports.</li> <li>• Understand the Prevent agenda and CONTEST.</li> <li>• Understand multiagency framework and Information sharing</li> <li>• Be able to raise concerns with the Safeguarding Team.</li> <li>• Puts into practice knowledge of how to reduce risks of harm.</li> <li>• Ability to contribute to meetings and or reports as necessary.</li> </ul>
Knowledge	<ul style="list-style-type: none"> <li>• As level 2. Understands the impact of Prevent on service users and their families</li> <li>• Be able to respond appropriately to concerns regarding possible Prevent issue</li> <li>• Knows the increased vulnerability of this group to radicalisation and grooming.</li> <li>• Understands issues around consent, confidentiality and the implications of data protection relevant to their own role.</li> <li>• Know who to share information with and when, understanding the difference between information sharing on individual, organisational and professional levels.</li> </ul>
Skills	<ul style="list-style-type: none"> <li>• Able to contribute to the assessment and implementation of care plans.</li> <li>• Able to identify and advise police and other professionals in respect of risk of radicalisation.</li> <li>• Able to communicate and engage effectively with service users and professionals regarding decisions affecting them as appropriate.</li> <li>• Able to identify the need for further specialist support, advice, and supervision in situations where problems require further expertise or intervention.</li> </ul>

**END**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROCEDURES FOR SAFEGUARDING SUPERVISION

**1.0 INTRODUCTION**

- 1.1 Working Together 2018 acknowledges that working to ensure children are protected from harm requires sound professional judgements to be made. The National Service Framework for Children Young People and Maternity Services 2004 advocates that *consistent, high quality supervision is the cornerstone of effective safeguarding of children.*
- 1.2 Supervision is defined by the Children's Workforce Development Plan 2007 as:  
  
'An accountable process which supports assures and develops the knowledge, skills and values of an individual, group or team. The purpose is to improve the quality of their work to achieve agreed outcomes'.
- 1.3 Many of the inquiries into child deaths, and serious incidents involving children, have demonstrated serious failings in professionals effectiveness which have been attributed to lack of 'supervised support' from professionals involved in the care of vulnerable children.
- 1.4 Trust staff working with children and adults are key professionals in the identification and prevention of abuse where there are safeguarding children concerns.
- 1.5 Trust staff should read this guidance in conjunction with the Trust Supervision and Appraisal Policy HR48 which outlines both clinical and management supervision arrangements.
- 1.6 Staff can access additional support and advice via the Workforce Wellbeing and Stress Management Policy (HR26).

**2.0 PURPOSE**

- 2.1 Supervision in safeguarding children is a formal process of professional support and learning, which enables and empowers practitioners to develop knowledge and competence, assume responsibility for their own practice and, therefore, enhance safeguarding children by assisting them to review, plan and account for their safeguarding work.
- 2.2 Supervision enables both the supervisor and the supervisee to reflect on, scrutinise and evaluate clinical practice and is both educative and supportive whilst facilitating the supervisee to explore their feelings about the work and the family. Safeguarding supervision aims to:
  - Ensure that clinical practice both protects and represents the best interest of the child.

- Provide a framework for supervisory practice, which enables the principles and underpins safeguarding supervision.
- Ensure that the respective roles, responsibilities and expectations of supervisor and supervisee are understood and agreed.
- Ensure that the boundaries of supervision are clear so that conflicts and confusion do not arise within this process.
- Establish a mechanism for evaluating the effectiveness of supervision.

2.3 Effective supervision enables the practitioner to:

- Keep a focus on the child.
- Avoid drift.
- Maintain a degree of objectivity and challenge fixed views.
- Test and address the evidence base for assessment and decisions.
- Address the emotional impact of work.

2.4 The key functions of supervision are:

- Management (ensuring competent and accountable performance/practice)
- Development (continuing professional development)
- Support (supportive/restorative function)
- Engagement/mediation

2.5 The process of supervision is underpinned by the principle that professionals remain accountable for their own practice and the Supervisor will be accountable for the advice and guidance given or action they take. All professionals should adhere to their professional code of practice.

2.6 All supervisors will have undertaken training in supervision.

2.7 Named Nurses and Specialist Practitioners providing supervision will themselves require specific supervision which can be accessed with similar colleagues and Designated professionals in accordance with local agreements.

2.8 Safeguarding Supervision will ensure that the racial, cultural, linguistic and religious identity of the child and family is consistently addressed for all families where there are child protection concerns.

## **3.0 PROCESS**

### **3.1 Confidentiality**

3.1.1 Supervision is a confidential process with the following exceptions. Information shared through the supervision process may need to be disclosed to another professional or agency in order to protect children from significant harm. Plans about the on-going and future work with the child and family will be documented in the child's health records and, therefore, those who acquire responsibility for the protection of the child in future will have access to that information.

- 3.1.2 If there are issues with regard to professional competence, unsafe or poor practice, which cannot be resolved within the supervisory relationship, this will be discussed with the practitioner, and a discussion taken as to how the issue will be resolved. This may involve consultation outside the context of supervision with the practitioner's line manager or named nurse. The outcome of these decisions will be recorded separate from the child's health records.
- 3.1.3 The safety and focus of individual children are the paramount consideration in any professional disagreement and unresolved issues should be escalated to a line manager with due consideration to the risks that may exist for the child.
- 3.1.4 If line managers are aware of professional concerns or personal circumstances that may impact upon a staff member's professional judgement and assessment of risk it is their responsibility to discuss this with their safeguarding supervisor. Best practice requires that this must be discussed with the member of staff prior to disclosure.

## **3.2 Structure**

- 3.2.1 Supervision is mandatory for all Trust staff and is monitored for compliance.

There are a variety of models used within the Trust area for safeguarding children supervision, including individual, group or peer supervision and pre and post case conference supervision. There are also different minimum standards for the frequency of supervision. For example, Mental Health staff must receive clinical and management supervision which includes Safeguarding, every 4-6 weeks. Community Health Services in Essex and Bedfordshire will require safeguarding children supervision two to four times per year.

- 3.2.2 The length of supervision session should be agreed between the health professional and the Supervisor/Named Nurse or Safeguarding team member to set clear parameters and allow the time available to be used to maximum effect, according to the individual needs of staff. Generally sessions should not exceed 2 hours.
- 3.2.3 Community Healthcare Teams may operate a clinical supervisor's model for safeguarding children supervision incorporating one to one and group supervision as reflected in National Society for the Prevention of Cruelty to Children (NSPCC) supervisors' programme. Those delivering Supervision will develop an agreement with the supervisee which will include frequency and venue as per agreed protocol. (See local Safeguarding Supervision agreements accessed via local Trust Safeguarding Teams).
- 3.2.4 Staff can access ad hoc supervision from the Safeguarding Team for support between formal/ planned individual and group supervision sessions.

### **3.3 Content and Documentation of Supervision**

3.3.1 Supervision will centre on children/families in the medium and high priority categories indicated by the National Assessment Framework tool as outlined in Appendix 3, Case Conferences Procedures. Additionally practitioners may bring to supervision cases regarding vulnerable children/families where there are difficulties in assessing the level of risk e.g. poor uptake of service, difficulty in gaining or engaging access, domestic abuse. The voice and lived experience of the child will be explored in case management supervision.

3.3.2 There should be a prepared agenda for the meeting in terms of casework and personal supervision. Plans that are formulated during supervision should be adhered to, with the targets set being realistic and in line with the practitioners own objectives. Issues that are identified in safeguarding children supervision should be responded to and acted upon.

3.3.3 The relevant client records should always be made available within the session. The appropriate Supervision forms, previously agreed action plans and priority lists where used should be used during supervision sessions.

3.3.4 The supervision discussion form enables an analysis of need to be made but will also constitute as evidence of supervision. Any specific health or safeguarding action plan should be entered in the child's or adult's record as appropriate. Any discussion form used will be, retained by both the practitioner and the Safeguarding team and will not be disclosed except for the purpose of a Local Child Safeguarding Practice Review formally known as a Serious Case Review, or disclosed by court order with a P.I.I. (Public Indemnity Immunity).

3.3.5 Records of supervision attendance must be maintained in accordance to the Trust supervision and appraisal policy for audit purposes.

3.3.6 Records of all case management discussions and care plans will contribute to the identification of trends and development and targeting of services for vulnerable children and families.

3.3.7 It is the Line Managers responsibility to identify where additional support is necessary for staff e.g. Complex cases, workforce issues or individual health professional need.

<b>END</b>
------------

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**PROCEDURE ON CHILD PROTECTION CONFERENCES**

**1.0 INTRODUCTION**

- 1.1 A Child Protection Conference (CPC) brings together family, child (where appropriate) and involved professionals. The purpose is:
- A Child Protection Case Conferences (CPC) brings together family, child (where appropriate) and involved professionals. The conference will analyse information on the child or children's development and needs and consider parents/carers capacity to response to those needs.
  - Consider information and evidence to make judgements about the likelihood of the child/children suffering significant harm or continuing to suffer significant harm.
  - Decide what future action is required in order to safeguard and promote the welfare of the child /children in relation to their future safety, health and development. If it is decided a protection plan is required this should also include a contingency plan if the agreed actions are not met.
- 1.2 A CPC can only be successful if staff work effectively in partnership and share information. This procedure gives guidance on preparation for Case Conferences and additional guidance on Child in Need/Partnership working and Looked After Children's meetings where relevant.
- 1.3 Trust staff will be expected to attend a CPC where they have a significant contribution to make arising from professional expertise or knowledge of the child, parent or carer.
- 1.4 This procedure is aligned to local children's services e.g. Trust Community Health Services (Essex) SGSOP3 for preparation for case conferences. This can be accessed on the Trust Intranet site.
- 1.5. If the conference decides that a child requires a Child Protection Plan a decision is made on the category of abuse e.g. sexual, physical, neglect, emotional. A Child Protection Plan will be formulated and regularly reviewed via a core group which includes relevant professionals, the child and family (where appropriate).
- 1.6. The Safeguarding Team are available for advice, support and debriefing sessions at all stages of preparation, decision making and resolving any professional disagreements in the process or developments of child protection plans.

<b>2.0 TIMEFRAMES</b>
-----------------------

- 2.1 An Initial CPC should be held within 15 days of strategy discussion where S47 enquiries were initiated. The first review conference must be held within three months of the initial conference and further reviews must be held at intervals of not more than six months, for as long as the child requires a child protection plan.
- 2.2 Pre Birth Conference involving an unborn child and must be conducted in the same manner as an initial CPC and should take place as soon as practical and at least ten weeks before the due date of delivery or earlier when there is a known likelihood of premature birth. A pre-birth conference should be held when a pre-birth assessment indicates risk of significant harm to the unborn, a previous child has died or been removed as a result of significant harm, children in the household or family are subject to a plan or as a result of an adult or child who is a risk to children resides in the house or is a regular visitor. A review conference must be scheduled to take place within one month of the child's birth. However this timescale may be extended to two months with the authorisation of Children's Social Care.
- 2.3 Where a child has transferred in from another area and required a child protection plan in that area then Children's Social Care is notified and a transfer conference should be held within 15 working days of the written notification of the move and request for transfer of case responsibility from the originating authority. The conference is then regarded as an initial CPC.
- 2.4 If a case conference is convened 'out of area' for a child receiving Trust services, a discussion with the Safeguarding Team must take place to ascertain if attendance is appropriate. The reason for non-attendance must be documented and follow up with the key worker following the conference must be recorded.
- 2.5 In some circumstances a child who is looked after may also be subject to a protection plan or be considered for a child protection conference. This would be as a result of:
- The child is subject to an Interim Care Order (ICO) and remains at home or is subject to proceedings without any order pending outcome of family court proceedings
  - The child is subject to a care order and is to be returned to their birth family/home.
  - The child is returned to parents/carers in court proceedings against the opinion of the local authority.
  - The child is looked after under section 20 of the Act and is about to be returned to parents care and there are concerns for the child's welfare.

<b>3.0 PROCESS</b>
--------------------

- 3.1 Staff attending a CPC should submit a case conference report two working days prior to an initial conference and at least 5 days prior to the review CPC. Staff should use the template recommended by their local area team or Local Safeguarding Partnership (available via the Trust Safeguarding site on the Intranet). Staff should be prepared to give an opinion about the category of abuse and contribute to the development & implementation of the plan. Case conference reports should include the relevant dimensions within the Assessment Framework as detailed in the safeguarding procedural guidance.
- 3.2 Staff should note that Case Conference reports can be added to Court Statements and they may discuss their CPC report with their line manager, Safeguarding Team or supervisor two weeks before review child protection conferences to allow time to produce the report within the specified timeframe.
- 3.3 All children should be seen by the named worker e.g. Health Visitor prior to a conference. If not seen a record of the reasons must be made. Staff should discuss the content of their report with the parents, and where appropriate, the child, and provide them with a copy at least 48 hrs before the conference. For review conferences this should be shared with parents and children at least five working days before the conference.
- 3.4 The report should be sent to the allocated social worker at least 5 days prior to the conference. In exceptional circumstances where insufficient notice has been provided for your attendance at conference it is acceptable for you to attend and provide a verbal report of your involvement.
- 3.5 It is important that staff working with the family attend conferences however if you are unable to attend a conference every effort must be made to find a colleague to attend in your absence. If you are unable to provide cover you must inform your line manager and send your report to the allocated social worker after sharing it with the parents. There may be instances where more than one health professional is involved with a family and invited to contribute to the case conference. In these circumstances and where appropriate one health professional can represent another, providing an appropriate briefing has taken place.
- 3.6 If you consider that a case conference may be difficult or complex, your operational line manager or a member of the Trust Safeguarding Team may attend with you to offer professional support.
- 3.7 If you disagree with a decision, you should voice your concerns at the time and make sure this is recorded in the minutes; this may prove important at a later date. Check case conference minutes carefully to ensure they are an accurate record of the conference. If you feel corrections are required, they should be forwarded to the Independent Review Officer (IRO) within ten working days of receipt of the CPC minutes.

- 3.8 A child who requires a child protection plan will not be allocated to a temporary member of staff. No newly qualified Health professional should be allocated child protection cases until they have completed training in Safeguarding Children. No newly qualified Health professional should undertake a first child protection case alone. A safeguarding supervisor, mentor or experienced practitioner preferably working in the same base should co-work the case with the newly qualified practitioner and attend the case conferences with the practitioner.
- 3.9 Good practice recommends that children who are subject to a child protection plan will retain their health practitioner when they change GP providing that the GP is located within a reasonable area. When the child is no longer subject to a child protection plan the child health records and care of the child can be transferred to the new GP's allocated health professional. This should be agreed in discussion with the family and safeguarding team and will take into account any continuing health needs and how these are best met. Consideration should be given to arranging a joint visit with the new health professional wherever practical.
- 3.10 A Community Healthcare Professional should be a member of the core group to represent the health care needs of the child or family and ensure they attend Core Group meetings accordingly.
- 3.11 Staff should follow their local arrangements regarding reporting the outcome of a conference in order to update relevant database and the Safeguarding team.
- 3.12 Staff attending CPC should ensure other relevant professionals working with the child or family are informed of the outcomes and relevant plans.
- 3.13 Copies of the CPC minutes and CP plan must be reviewed by the health professional in attendance of the CPC and inserted into the child's records. If recorded on an electronic record they must be labelled with the date of the conference. Health professionals attending the CPC must comply with Trust contemporaneous record keeping, by recording their attendance and the salient points and outcomes of the CPC in the child's health record.
- 3.14 Core Group:**
- 3.14.1 The initial Core Group is held within ten days after the conference and then Core Groups typically take place every 6 weeks. Trust staff should consult the relevant procedures within the Local Safeguarding Partnership guidance for the area in which they work.
- 3.14.2 The focus of the Core Group is the implementation and monitoring the effectiveness of the Child Protection Plan to deliver positive impact for the individual child. Staffs are responsible for participation in Core Group meetings. Staffs take responsibility to action their specific element of the Child Protection Plan, continually assessing the effectiveness of the plan, and challenging drift.

3.14.3 Health professionals will be expected to assist their social care colleagues, by taking the minutes or chairing the core group meetings. Children's social care will retain ownership and responsibility to circulate the core group minutes.

3.14.4 Copies of the Core Group minutes and updated CP plan must be reviewed by the health professional in attendance of the Core Group and inserted into the child's records. If recorded on an electronic record they must be labelled with the date of the meeting. Health professionals attending the Core Group must comply with Trust contemporaneous record keeping, by recording their attendance and the salient points and outcomes of the Core Group meeting in the child's health record.

### **3.15 Partnership Meetings:**

3.15.1 Where there are concerns for a child a partnership meeting can be arranged by staff to assess needs and identify any risks. All meetings should include parents/carers, the child (where appropriate) and relevant professionals invited to attend.

3.15.2 The key worker for the family would normally chair such meetings but this may be allocated to another relevant professional where agreed. All such meetings must be recorded and copies of minutes should be sent to all attendees including parents.

3.15.3 If a parent fails to attend then the chair person should discuss the meeting with the parent and send a copy of the minutes.

3.16.3 In exceptional circumstances partnership meetings without parents/carers/child's knowledge, may need to be considered.

<b>4.0 TRANSFERRING RECORDS OF CHILDREN WHO HAVE A CHILD PROTECTION, CHILD IN NEED PLAN OR WHO ARE LOOKED AFTER</b>
---

4.1 When families move frequently, it is more difficult to monitor a child's welfare and identify any risks. Staff must be alert to the possibility that a child or family who comes to their attention may not be in receipt of universal services. All staff that comes into contact with families, who have moved, must ensure that they establish basic information regarding full names, dates of birth, previous address, registration with doctor and the child's enrolment in school.

4.2 Transferring records should comply with the Trust record keeping guidance. Staff should note the importance of transferring relevant records and information as soon as possible.

4.3 Where there are children subject to a Child Protection Plan, Child in Need, LAC or high level domestic abuse case, staff must discuss the case with the relevant member of staff in the receiving area/team within 3 working days and records should be sent within 5 working days. Staff should also inform the;

- Child Health Information Service and Social Care as appropriate.
- Allied health professional and GP as appropriate.

4.4 Staff must ensure that any significant events sheet used reflects the latest information including the change of address and other relevant information. Additionally Community Health Service staff may need to complete an electronic records transfer summary sheet in full, clearly identifying any forthcoming appointments and meetings as well as the care plan and outstanding actions.

#### **4.5 Transfer out of the Trust area**

4.5.1 Where staff are aware that a child has moved, it is the responsibility of health in the originating authority, prior to the child's move, to provide information to their colleagues in the receiving authority. If this information has not arrived by the time the child moves, it is the responsibility of health in the receiving agencies (once they become aware of the child's arrival) to request the information is received within five working days.

4.5.2 If a member of staff discovers that a child who is the subject of a child protection plan is planning to move, or has moved out of / into the area they should inform Children's Social Care immediately, and confirm this information in writing on the same day. Social Care will then inform relevant other agencies and professionals involved in the case.

4.5.3 Records for transfer out should be recorded on appropriate systems and sent with any paper records and electronic print outs to the relevant health professional or child health department.

#### **4.6 Transfer into Trust area**

4.6.1 Health Visitor/ School Nurse and FNP records received into the child health services should be forwarded directly to the practitioner if indicated within the record. For records where the practitioner is not indicated the child health department will forward these to the team manager for the nearest base to the address or school indicated in the records for allocation. If a practitioner receives a record direct from the originating authority they must contact the child health department and notify them of the transfer details.

<b>END</b>
------------

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROCEDURES FOR RESPONDING TO DOMESTIC ABUSE and DOMESTIC  
INCIDENT REPORTS

1.0 INTRODUCTION

1.1 This procedure offers guidance on Domestic Abuse which includes

- Coercive control
- Female Genital Mutilation
- Forced Marriage and Honour Based Abuse
- Hate Crime

1.2 The Home Office 2013 updated the definition of domestic violence and abuse to reflect that many young people are experiencing domestic abuse and violence in relationships at a young age and may therefore be Children in Need or likely to suffer significant harm. Domestic abuse is defined as:

*“Any incident or pattern of incidents of coercive, controlling and threatening behaviour, violence or abuse between those aged 16 or over who are, or have been intimate partners or family members, regardless of gender or sexuality”.*

The abuse can encompass;

- Psychological
- Physical
- Sexual
- Financial
- Emotional

1.3 In December 2015 the offence of Coercive Control came into force in England and Wales.

Coercive behaviour, is an act or pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish or frighten their victim

Controlling behaviour is a range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating their everyday behaviour.

1.4 Prolonged and/ or regular exposure to domestic abuse can have a serious impact on children’s safety and welfare, despite the best efforts of parents to protect them. An exploration of the possible impact on the unborn child shows the foetus is at risk of injury because violence towards women increases both in severity and frequency during pregnancy, and often involves punches or kicks directed at the women’s abdomen.

## **CLPG37 - SAFEGUARDING CHILDREN PROCEDURE**

### **APPENDIX 4**

- 1.5 All children living in a household where there is domestic abuse will be affected. Those children that witness domestic abuse can be significantly affected both emotionally and behaviourally and suffer physical abuse.
- 1.6 Both men and women can be victims of domestic abuse though a greater proportion of women experience all forms of domestic abuse and are more likely to be seriously injured or killed by their partner or ex- partner.
- 1.7 Domestic incident reports are produced by the police and distributed to Community Healthcare services and some mental healthcare services within the Trust when an incident occurs involving a family where children are likely to or known to be present.
- 1.8 In April 2011 Domestic Homicide Reviews (DHRs) were established on a statutory basis under section 9 of the Domestic Violence, Crime and Victims Act (2004). A DHR review means a review of the death of a person aged 16 or over has, or appears to have, resulted from violence, abuse or neglect by:
  - A person to whom he was related or with whom he was or had been in an intimate personal relationship, or
  - A member of the same household as him/herself,

The purpose of a DHR will be to identifying the lessons to be learnt from the death and relevant Trust Staff involved will be required to discuss the case with the identified member of staff conducting an Individual Management Review. Further guidance on the procedure for DHR is available in the Trust Safeguarding Adult Procedure CLPG39 Appendix 3.

## **2.0 PURPOSE**

- 2.1 This procedural guidance supports the three central imperatives of intervention for children living within domestic abuse and violence which are:
  - To protect the child or children including an unborn.
  - To empower the victim/ to protect her/himself and the children.
  - To identify the abusive partner.

## **3.0 PROCESS**

- 3.1 The Trust has different processes in place for responding to Domestic Incidents in accordance to the local police departments arrangements. Therefore staff should follow the general process below but be aware of specific process for their areas of work. Staff should contact their Safeguarding Named professional for advice if they are unclear or access the Safeguarding Intranet site

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 4**

- 3.2 Staff should be able to recognise indicators and know how to respond to domestic abuse to safeguard children and the victim. When domestic abuse is identified staff should:
- Focus on the victim's safety and that of their children.
  - Share relevant information and refer if required to relevant agencies e.g.GP, Social Care.
  - Support and reassure the victim.
- 3.3 When talking to an individual about domestic abuse staff should **never**:
- Discuss the situation or potential risk when another person is present.
  - Promise confidentiality if there are children in the family.
  - Accept culture as an excuse for domestic abuse.
  - Force the victim to make a disclosure.
  - Encourage them to immediately leave the family home.
- 3.4 If a referral to social care is required staff should inform the parent, unless it is felt that this may cause additional risk of harm to the victim or a child.
- 3.5 Where there is evidence of domestic abuse, the implications for any children in the household must be considered and a referral to Children's Social Care **must** be made where staff are aware of;
- A child's direct involvement with a domestic abuse incident or injury;
  - A victim who is a woman and is pregnant. Pregnant women frequently experience punches and kicks directed at the abdomen, risking injury to both mother and foetus;
  - Any child injured during episodes of violence or is witnessing the physical and emotional suffering of a parent.
- 3.6 Where an interpreter is required, **never use a family member** as in cases of honour based violence there is a high likelihood that this will increase the risk of serious harm to the victim and children
- 3.7 Where there are no Safeguarding children concerns and the person requests that no further action should be taken regarding domestic abuse then staff must
- Decide if the person has capacity to make an unwise decision.
  - Consider risks to others including other family members.
  - Advise on support services available.
- 3.8 Victims of Domestic Abuse may remain with an abusive partner for many years whilst suffering abuse without considering leaving or sometimes not recognising that they are living within an abusive relationship.

Staff must consider the welfare of any child or another adult where there are additional areas associated with domestic abuse. Including the below.

### 3.9 Female Genital Mutilation

3.9.1 Female Genital Mutilation (FGM) is known by a variety of names including 'Female Genital Cutting', 'Circumcision' or 'Initiation'. However FGM is the most recognised name used by professionals and community settings.

3.9.2 FGM is prevalent in 30 countries concentrated around Africa, Middle East and some countries in Asia. It has also been identified in Europe, North America and Australia.

#### **The practice is NOT required by any religion**

3.9.3 FGM is a form of violence against women and girls which is in itself both a cause and consequence of gender inequality. As such it can be associated with other discriminatory forms of honour based violence including forced marriage and domestic abuse.

3.9.4 FGM is defined as the removal of part or all of the female genitalia for non – therapeutic reasons. It is frequently a very traumatic and violent act for the victim and can cause severe pain, mental health problems, genito urinary problems and difficulties in childbirth.

3.9.5 FGM is illegal in the UK. It is a criminal offence not only in the UK but includes taking a child abroad to undergo FGM, whether or not it is lawful in that country.

3.9.6 The FGM Act 2003 states that health professionals have a **mandatory duty** report known or potential cases of FGM in under 18's to social care and the Trust Safeguarding team.

3.9.7 A child for whom FGM is planned is likely to suffer significant harm through physical abuse and emotional abuse, which is categorised by some also as sexual abuse.

3.9.8 Health professionals encountering FGM should be alert to the risk of FGM for siblings, daughters and /or extended family members.

### 3.10 Honour Based Violence

3.10.1 Honour Based Violence is committed against someone who is perceived to have brought shame or dishonour on a family or even a community. Incidents that have preceded honour killing have included:

- Attempts to separate or divorce.
- Threats to kill or denial of access to children.
- Pressure to go abroad and forced marriage.

3.10.2 A child who is at risk of Honour Based Abuse is at significant risk of physical harm including being murdered. Staff suspecting Honour Based Abuse should refer to social care and the Trust Safeguarding Team. They should NOT discuss with family members.

3.10.3 Accurate record keeping is essential when managing a case involving honour based abuse. Practitioners should ensure that they use the child's words verbatim, date and time the details and make note of any injuries using body maps where indicated.

3.10.4 It is important to see the child on their own even if they are accompanied by others and establish a mechanism of contacting them discreetly in the future.

### **3.11 Forced Marriages**

3.11.1 In June 2014 it became a criminal offence to force someone to marry. A child who is being forced into marriage is at risk of significant harm from physical, sexual and emotional abuse.

3.11.2 Warning signs include:

- Family history of an older sibling leaving the country suddenly or marrying early.
- Anxiety, depression or emotionally withdrawn.
- Absence from school or other regular activity.
- Fear of forthcoming visits to their country of origin.
- A child going missing/running away.
- A child talking about an upcoming family holiday they are worried about.
- Surveillance by family members especially siblings.
- A child directly disclosing that they are worried s/he will be forced to marry.

3.11.3 Staff suspecting Forced Marriage should contact Social Care and the Trust Safeguarding Team immediately. They should not approach or discuss with the family. Staff should follow the same guidance as indicated for Honour Based abuse in relation to record keeping and seeing the child alone.

### **3.12 Hate Crime/Incidents**

Hostility or prejudice towards an identifiable group of people (race, religion, disability or sexual orientation). Incidents often involve physical assault, bullying, hate mail. Where there may be risks to other adults from the perpetrator then staff should consider a Safeguarding Adult Referral (Trust Safeguarding Adult Procedure CLPG39).

### **3.13 Spiritual Possession and Witchcraft**

Children are at risk of harm where parents, families and the child themselves believe that an evil force has entered a child and is controlling them, the belief includes the child being able to use the evil force to harm others. Parents can be initiated into and/or supported in the belief that their child is possessed by an evil spirit. A child may suffer emotional abuse if they are labelled and treated as being possessed with an evil spirit. In addition, significant harm to a child may occur when an attempt is made to 'exorcise' or 'deliver' the evil spirit from the child.

## **4.0 DOMESTIC INCIDENT REPORTS DIR**

- 4.1 There are separate domestic abuse protocols within Children's Community Health Services that relate to the process for Domestic Incident Reports (DIR). DIR are sent electronically by the police to Trust Safeguarding Children Teams via secure NHS mail account. Some are also sent to Children's Social Care.
- 4.2 A copy of the DIR will be distributed to the named professional e.g. health visitor, school nurse. Staff must ensure the information is assessed against the child or parent records and an action plan developed if required. A copy should be filed within the child or adults record where appropriate and in accordance to local protocol.
- 4.3 All DIR received involving pregnant women are distributed to the relevant midwife or hospital as per the protocol for Information sharing in respect of domestic abuse involving a woman in the antenatal period.
- 4.4 Staff receiving DIR will discuss with other relevant staff in order to safeguard the unborn or other relevant children or adults. A discussion with GP and relevant mental health professional should take place to share information and establish if there are any additional concerns.
- 4.5 Community Health Practitioners will prioritise the actions they take based on
- The number of incidents.
  - There is a current or previous child protection plan.
  - The incident has been identified as high or very high risk by the police.
  - The child is subject to a child in need plan.
  - Pregnancy.
  - Knowledge of the family and any previous concerns.
- 4.6 Some DIR's are notified to social care by the police however staff should not assume that Social Care will have all information regarding the child or family. If a DIR is received for the criteria above then staff should contact Social Care to establish any action to be taken by all involved professionals.

- 4.7 Caseload holders must record all incidents using the appropriate forms (e.g. Chronology of Events /selective intervention template) used by teams. This must include the nature of the incident, the assessment of its impact on the child or young person and the resulting action plan.
- 4.8 Where a DIR is received and a school child attends a school out of area then the Safeguarding Team will forward the DIR to their counterpart team in the relevant area.
- 4.9 When a DIR is received and the parent/child is not registered with a GP then the relevant professional should be notified in the geographical area that the child/parent is resident.
- 4.10 The Safeguarding Children team will provide supervision on cases where the practitioner has concerns for the impact of the domestic abuse on the child or young person.

<p><b>5.0 DOMESTIC ABUSE STALKING &amp; HARASSMENT (DASH) RISK ASSESSMENT &amp; MULTI AGENCY RISK ASSESSMENT CONFERENCE (MARAC)</b></p>
---

- 5.1 Where staff have concerns regarding a victims safety following the receipt of a domestic incident a DASH risk assessment tool can be used to help aid a discussion between staff and victim and assess the level of risk to victim and any others including children. The DASH tool is available via the Trust Safeguarding Intranet site.
- 5.2 Where a DASH has been completed and reaches the threshold (14 ticks) or where professional judgement dictates, then a referral to the Multi Agency Risk Assessment Conference (MARAC) by the practitioner or the Trust local representative or Domestic Abuse Lead.
- 5.3 MARAC meetings are attended by local representatives from organisations which may be involved in supporting victims, or working with the perpetrator. MARAC's occur regularly (monthly or more frequently) across the Trust area and are chaired by police.
- 5.4 The purpose of a MARAC is to share information about Very High Risk victims in order to prevent serious harm, develop a safety plan, put all possible support in place and lower the risk to children and victim as soon as possible.
- 5.5 The Trust is represented at MARAC by identified senior practitioner e.g. Care Co-ordinators, Criminal Justice Teams and Specialist Community Health service staff.

- 5.6 All staff attending MARAC should provide information to aid assessments and reduce risk. Staff should check with Children's Social Care that any child or unborn is known and if not a referral should be made.
- 5.7 Most MARAC will have an Independent Domestic Violence Advocate (IDVA) who is able to act as a bridge between the victim and the MARAC meeting and act as the primary point of contact for the victim. And offer support during any court proceedings.

## **6.0 RECORD KEEPING**

- 6.1 It is important that staff follow the Trust, and local team record keeping policy and procedure. All actions and reasons for not taking action should be recorded clearly.
- 6.2 Staff should note that any Trust records containing information on domestic abuse may be used for:
- Criminal proceedings.
  - Civil proceedings regarding contact arrangements between perpetrators and children.
  - Domestic Homicide Reviews.
  - Housing provision.

**END**

**ESSEX PARTNERSHIP UNIVERISTY NHS FOUNDATION TRUST**

**PROCEDURE ON THE WELFARE OF UNBORN BABIES**

**1.0 INTRODUCTION**

- 1.1 This procedural guidance is relevant to staff working directly with families, pregnant women or young people for the purpose of safeguarding the unborn baby. This guidance should be read in conjunction with the LSCB Pre Birth procedures for the geographical area where the child and family are resident
- 1.2 Where agencies or individuals anticipate that prospective parents may need support services to care for their baby or that s/he may be at risk of significant harm, a referral to Children's Social Care must be made at the earliest opportunity and preferably before 28 weeks gestation to allow for a pre-birth assessment to take place . Referral must always be made in any of the following circumstances:
- There has been a previous unexpected or unexplained death of a child whilst in the care of either parent.
  - A parent, adult or other regular visitor in the household is a person identified as presenting a risk, or potential risk, to children.
  - Children in the household / family currently subject to a child protection plan or previous child protection concerns.
  - A sibling (or other child in the household of either parent) has previously been removed either temporarily or by court order.
  - There is knowledge of parental risk factors including mental illness, domestic abuse, substance misuse and it is considered that these issues may impact significantly on the baby's safety or development.
  - Concerns exist about parental ability to self-care and/or to care for the child e.g. unsupported young or learning disabled mother.
  - There are maternal risk factors e.g. denial of pregnancy, avoidance of antenatal care (failed appointments), non-co-operation with necessary services, non-compliance with treatment with potentially detrimental effects for the unborn baby.
  - Any other concern exists that the baby may be at risk of significant harm including a parent previously suspected of fabricating or inducing illness in a child.
  - Late presentation of pregnancy with concerns that the parents have attempted to conceal the pregnancy for any reason.
  - A child aged under 13 is found to be pregnant

1.3 Where the concerns centre around a category of parenting behaviour e.g. substance misuse, the referrer must make clear how this is likely to impact on the baby and what risks are predicted. Delay must be avoided when making referrals in order to:

- Provide sufficient time to plan for the baby's protection.
- Provide sufficient time for a full and informed assessment.
- Avoid initial approaches to parents in the last stages of pregnancy, at what is already an emotionally charged time.
- Enable parents to have more time to contribute their own ideas and solutions to concerns and increase the likelihood of a positive outcome to assessments.
- Enable the early provision of support services so as to facilitate optimum home circumstances prior to the birth.

Concerns should be shared with prospective parent/s and consent obtained to referral unless this might place the welfare of the unborn child at risk. Consideration should be given to holding a strategy meeting/discussion when the parent is a looked after child.

#### 1.4 **Process**

1.4.1 Staff in contact with pregnant women should routinely assess the needs of the unborn baby. Where it is indicated that prospective parents may need support services to care for their baby a referral to Children's Social Care must be made as early as possible. However if there are concerns for the safeguarding of the unborn baby then Community Healthcare professionals or other relevant staff should make a referral to Children's Social care immediately. Children's Social Care should undertake a Single Assessment, unless this has already been undertaken by the referrer. There is a defined period for completion of the Single Assessment, which is 45 days in total, with a review point at 20 days, it is expected that the majority of these assessments will conclude at 45 days in order for a full and thorough assessment to be completed. The aim is always to conclude where possible the pre-birth assessment to enable child in need planning to Pre-Birth Assessment Multi-agency protocol by around 27-30 weeks of the pregnancy. A birthing plan will need to be shared with the multi-agency professionals prior to the birth.

1.4.2 If the assessment does not indicate that the baby will be at risk of significant harm when born but may be a child in need, then the planning and provision of services will continue under s17 of the Children Act 1989. If, however the assessment does indicate that the baby will be at risk of suffering significant harm then a Child Protection Conference will be held at 30 weeks gestation. If it is not necessary for the Local Authority to provide services under s17 or 47 of the Children Act professionals can still have a multi-agency meeting to bring together all professionals involved with the family and establish a plan of how best to support the family.

- 1.4.3 The Child Protection conference and any subsequent reviews will proceed as per all other conferences, the first review being held within 4 weeks of the baby's birth or in exceptional circumstances within 3 months with the approval of the responsible Social Work team manager and Child Protection Co-ordinator. This will include relevant members of staff e.g. health visitor, Community Drug & Alcohol (CDAS) staff and the Perinatal Mental Health Team. If the decision is made to proceed with a child protection plan for the unborn child, then the name ("Unborn" mother's name) and the due date of delivery should be entered on all electronic and hard copy records. The baby's record should be linked with the mother's record.
- 1.4.4 The core group should meet before the birth, and also before the baby is discharged from hospital. The Core Group record should highlight the:
- Outcome of assessment;
  - Pre / post birth plans, including Child Protection Plan;
  - Managing non co-operation;
  - Removal at birth – if the plan is to remove the baby at birth, plans must be in place to fulfil the statutory requirements relating to Looked After Children and the preparation of foster carers if any post-birth health needs are likely.
- 1.4.5 Detailed written plans need to address:
- Who should hospital contact when mother is admitted / in labour / baby delivered?
  - Who will give consent for screening?
  - What happens if baby is born out of hours?
  - What level of contact / care (supervised or not) can the parents have, and who will assume responsibility for supervising care/contact?
  - What is the plan in relation to breast-feeding?
  - What needs to be in place for baby to go home?
  - Where will baby go home to?
  - Which professionals need to visit?
  - Which day is each person going to visit?
  - Does the child need to be seen every day or is it necessary to do an unannounced visit, and what is the contingency plan?
  - What family support needs to be in place?
  - What have family members agreed to do?
  - Is the family part of the visiting schedule?
  - Are the parents aware of the plan & what is their presentation/attitude?
  - Possible family arrangements for care of the baby
  - Expectations and process for reporting concerns in and out of working hours
  - How long the plan is in place for and when it will be reviewed?
  - What are the arrangements for initiating legal proceedings?
  - The intensive support required for mother and baby to live in the community, and any other specialist assessments

1.4.6 For families where Staff are aware of parental misuse of drugs or alcohol, this becomes relevant to child protection when the misuse of the substances impacts on the care provided to their children. Substance misuse may include experimental, recreational, poly-drug, chaotic and dependent use of alcohol and / or drugs. Over the counter medication as well as prescribed/illicit drug use can be very potent if combined.

Misuse of drugs (prescribed and illegal) and/or alcohol is strongly associated with significant harm to children, especially when combined with other features such as domestic violence, mental illness. Non-compliance with treatment may also indicate a potential risk to children in the family.

1.4.7 A referral to children's social care must always be made when:

- Substance misuse is combined with domestic abuse or mental illness.
- The substance misuse of a parent or carer is chaotic or out of control.
- Drugs and paraphernalia (e.g. needles) are not kept safely out of reach of children.
- Children are passengers in a car whilst a drug or alcohol misusing carer is driving.
- Where both parents are drug / alcohol abusing, and there is a lack of positive social support/network.

1.4.8 Trust staff working with pregnant women or family members must routinely work in partnership across agencies e.g. midwifery, social care, CDAS, Perinatal Mental Health team, Health visitors, GP and services to ensure an effective assessment of risks, needs and identify if there are other children in the household.

1.4.9 Trust Community Healthcare Professionals working with a woman or young person who is substance misusing during pregnancy should seek to support and manage their care and consider the likely implications of their substance misuse on their unborn child. Relevant staff should attend multi-agency meetings held upon invitation or make arrangements for a colleague to attend if they are not able. The health professional will make contact with the woman or young person during her pregnancy to explain the service and an early help assessment can be completed if required for an assessment of needs for the mother, the unborn and any other relevant person in the household. This will then inform the care plan of any pre-birth contact to be made in partnership with the family.

<b>END</b>
------------

ESSEX PARTNERSHIP UNVERISTY NHS FOUNDATION TRUST

PROCEDURES FOR SAFEGUARDING CHILDREN IN WHOM ILLNESS IS  
FABRICATED OR INDUCED

1.0 INTRODUCTION

- 1.1 This procedure outlines the procedures to follow when staff are concerned that the health or development of a child may be significantly impaired by the actions of a parent or carer having fabricated or induced illness.(FII)
- 1.2 This procedure should be read in conjunction with the below which is available on the Trust intranet.
- Local Safeguarding Children's Board guidelines and the DoH Revised Guidance 2008.
  - The Royal College of Pediatrician's and Child Health 2009 *Fabricated or Induced Illness by Carers* provides further guidance for medical staff
- 1.3 Staff should be aware that there are a number of local Operational Procedures regarding FII that link to this overarching procedure. These should also be referred to and are available on the trust intranet or via the Safeguarding team.

2.0 DEFINITION

- 2.1 Fabricated or Induced Illness (FII) in a child is a condition whereby a child suffered harm through the deliberate action of the parent usually mother or female carer and which is duplicitously attributed by the adult to another cause
- 2.2 There are 3 main and not mutually exclusive ways of the parent/carer fabricating or inducing illness:
- Fabrication of signs and symptoms, including fabrication of past medical history;
  - Fabrication of signs and symptoms and falsification of hospital charts, records, letters, documents and specimens of bodily fluids;
  - Induction of illness by a variety of means.
- 2.3 Harm to the child may be caused through unnecessary or invasive medical treatment, which may be harmful and possibly dangerous, based on symptoms that are falsely described or deliberately manufactured by the parent/carer, and lack of independent collaboration.

The child may additionally suffer emotional harm through the limitations placed on their development and social interaction e.g. prevention from participation in normal activities.

### **3.0 RECOGNITION OF EMERGING CONCERNS**

- 3.1 FII should be suspected if a child's history, physical or psychological presentations or investigations lead to a discrepancy with a recognised clinical picture and one or more of the following is present:
- Reported symptoms and signs found on examination are not explained by any medical condition;
  - Results of investigations do not explain reported signs and symptoms;
  - Inexplicably poor response to prescribed medication and treatment and the parent/carer appears to know a lot about the medication and treatment;
  - New symptoms reported on resolution of previous ones;
  - Over time the child repeatedly presents with a range of symptoms;
  - Child's normal daily life activities are being curtailed;
  - The attendance at various hospitals, in different geographical areas;
  - Carers may be over involved in participating in medical tests;
  - Taking temperatures and measuring bodily fluids;
  - Reported symptoms are only observed by the parent/carer and only appear or reappear when they are present;
  - There is a history of events that are biologically unlikely;
- 3.2 Staff working with the child may notice discrepancies between reported and observed medical conditions.
- 3.3 Trust Staff working with the parent/carer may also note relevant concerns e.g. the child being drawn in to the parent's mental illness.
- 3.4 Trust Staff working with parents where it is felt the parent is fabricating illness should always consider the welfare of children.
- 3.5 Generally some indicators of abuse (often in the context of wider parenting difficulties) may (or may not) be associated with this form of abuse such as:
- Non organic failure to thrive.
  - Speech, language or motor developmental delays.
  - Dislike of close physical contact.
  - Attachment disorders.
  - Low self-esteem.
  - Poor quality or no relationships with peers because social interactions are restricted.
  - Poor attendance at school and under-achievement.
  - Child's carers may have history of abuse and/or psychiatric illness.

### **4.0 STAFF RESPONSE**

- 4.1 Trust Staff who have concerns about a child with suspected FII should discuss the case with their line manager and Trust Safeguarding Team. An early discussion should take place with the child's GP and where relevant paediatrician.

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE**  
**APPENDIX 6**

- 4.2 Diagnosis of FII can be very difficult because the reported signs and symptoms cannot be confirmed when they are being exaggerated or imagined, or maybe inconsistent when they are being induced or fabricated.
- 4.3 Where FII is suspected staff should check if parent is also known to Trust services. The practitioner should record the health concerns within the child's health records so other clinicians can access this. With support from the safeguarding team the professional will arrange an initial professionals meeting within 10 days of the initial identification of concerns.
- 4.4 The responsible paediatrician will lead this meeting and all health professionals involved in the child's care should attend along with the Designated Nurse. In cases where there is not a paediatrician the Designated Doctor will lead this meeting. A chronology of involvement with child or parent will be required and the template for this will be shared by the commissioning safeguarding team for the practitioner to complete and return. A composite chronology will then be shared with the Designated Paediatrician or Doctor. The responsible paediatrician will then arrange for a medical evaluation to take place and if no paediatrician is known to the child a referral will be made from the GP to allocate a paediatrician.
- 4.5 Where the consultant has reasonable cause to suspect that the child is suffering or is likely to suffer significant harm a referral to Children's Social Care will be required which clearly outlines the specific concerns. The parents should **NOT** be informed that a referral is being made. The police child abuse investigation team will also be informed of any referral where FII is suspected as this may also involve a crime.
- 4.6 Children's social care will arrange a strategy meeting to gather information; this meeting will involve police and all other relevant professionals. In such cases, parents must **NOT** be informed of the meeting or professionals concerns of FII at this stage.
- 4.7 The outcome of the strategy meeting will set out the immediate plan to protect the child, which may include admission of the child/children to hospital for observation. A second professional meeting with the Designated Doctor and other health professionals may also be arranged to discuss the outcome and any further action required.
- 4.8 Trust staff attending a Case Conference must prepare a Case Conference report and any supporting information e.g. chronology of involvement.
- 4.9 If staff feel they need to escalate their concerns regarding, professional difference of opinion they must consult with the Safeguarding Team and follow the local LSCB escalation protocol.

<b>END</b>
------------

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST****PROCEDURE GUIDELINES FOR SAFE WORKING PRACTICE WITH CHILDREN  
& MANAGING ALLEGATIONS AGAINST PEOPLE WHO WORK WITH CHILDREN****1.0 ALLEGATIONS AGAINST STAFF WORKING WITH CHILDREN****1.1 Introduction**

These procedures comply with *Working Together 2018* and the Local Safeguarding Children Board guidance. They should be applied in conjunction with the Trust HR policies and the LSCB Safeguarding Children Procedures. These procedural guidelines will enable staff to recognise and take appropriate action when there is an allegation against people who work with children.

1.2 The Department of Health document *Working Together to Safeguard Children 2018* states that all organisations that provide services for children and young people up to the age of eighteen years should operate a procedure for handling allegations of abuse or maltreatment against staff and have a Senior Officer responsible for managing allegations.

1.3 The Designated Senior Manager is the Executive Medical Director.

1.4 The Designated Senior Manager should work closely with the Local Authority Designated Officer (LADO) to ensure that any allegation of abuse is dealt with fairly, quickly and consistently to provide effective protection for the child and at the same time supports the member of staff subject to the allegation.

1.5 An allegation may require consideration from any of the following inter-related perspectives:

- Child protection enquiries by Children's Social Care;
- Criminal Investigation by the Police;
- Staff disciplinary procedures;
- Complaints procedures.

1.6 Data on LADO referrals will be reported to the relevant Clinical Commissioning Group (CCG) as required.

**2.0 SCOPE**

2.1 This procedure applies to all staff including temporary or voluntary sector staff whenever it is alleged or there is a concern that they have:

- Behaved in a way that has or may have harmed a child;
- Possibly committed a criminal offence against or related to a child; or
- Behaved toward a child in a way which indicates s/he would pose a risk of harm to children.

2.2 If concerns arise about a member of staff's behaviour toward their own children, Children's Social Care and/or Police will consider informing the

Trust in order to assess whether there may be implications for children with whom the person has contact at work.

- 2.3 If an allegation in relation to a child is made about a member of staff who works with adults, consideration must be given to alerting the named Senior Officer.

### **3.0 ROLES & RESPONSIBILITIES**

3.1 The Designated named Senior Officer who is the Senior Manager is the Executive Medical Director.

3.2 The Designated named Senior Officer is responsible for:

- Ensuring the Trust operates procedures in accordance with Working Together 2018 and local Child Protection procedures;
- Resolving any inter-agency issues;
- Liaises with the Local Authority Designated Officer (LADO)

3.3 Each Local Authority will have a particular officer previously known as Designated Officer or LADO who is responsible for:

- Providing advice and guidance to the Trust;
- Liaise with Police and other agencies;
- Monitor the progress of cases.
- Be involved in the management, co-ordination and oversight of cases.

### **4.0 CONFIDENTIALITY**

4.1 Enquiries must be conducted in the strictest confidence to ensure information is given freely and in a way that protects the rights of all concerned. Every effort should be made to maintain confidentiality and guard against publicity whilst an allegation is being investigated or considered.

4.2 Information about an allegation must be restricted to those who have a need to know in order to protect children, facilitate enquiries and manage the disciplinary/complaints process.

### **5.0 REPORTING ALLEGATIONS**

5.1 Any allegation of abuse must be reported to the Line Manager, Safeguarding team or directly to the Designated Senior Manager immediately.

5.2 The Line Manager and safeguarding team must report any allegations to the Designated Senior Manager.

5.3 A record of the report must be made which includes time date, place, people present and what was said. A clear signature is required in accordance with the record keeping policy.

- 5.4 The Trust Designated Senior Manager must inform the Local Authority Designated Officer of all cases that meet the criteria in paragraph 2.1 within one working day and prior to any further investigation having taken place so that consultation with or referral to the Police or Children's Social Care can take place as appropriate. If an allegation requires attention immediately and is outside of normal working hours, the Local Authority emergency duty team or police should be contacted and followed up with the LADO during the next day's normal working hours.
- 5.5 The Trust Designated Senior Manager will seek advice from the Local Authority Designated Officer if informing the parents/carer of the child if relevant will impede the disciplinary or investigative process. The outcome may involve the information being either fully or partially shared with the parents. The Trust Designated Senior Manager should inform the accused person about the nature of the allegation, how enquiries will be conducted and the possible outcome (e.g. disciplinary action, and dismissal or referral to the DBS or regulatory body). This will be subject to the restrictions of the information that can be shared.

## **6.0 MANAGING ALLEGATIONS**

- 6.1 The Trust Designated Senior Manager will be responsible for sharing relevant information about the allegation, child and accused member of staff with other relevant agencies involved. As soon as possible after an allegation has been made the accused member of staff should be advised to contact their union or professional representative.
- 6.2 Support should be made available by the most appropriate person to the child/ren by considering the impact upon them and to address the child's needs. The accused member of staff should equally be advised to contact their union or professional association and Human Resources should be consulted so that the appropriate support can be provided by Occupational Health.
- 6.3 A Management Planning meeting should be arranged with the LSCB Designated Officer, Police and Child Protection Service Manager to chair the meeting. Additional members may include Human Resources manager, Trust Safeguarding Team etc. as appropriate.
- 6.4 The Planning meeting will consider the course of action needed to protect and support the child and the action to be taken for the member of staff. It will additionally use the following definitions to determine the outcome of allegation investigations:
- Substantiated: Sufficient identifiable evidence to prove allegation
  - False: Sufficient evidence to disprove the allegation
  - Malicious: Clear evidence there has been deliberate act to deceive and allegation is false
  - Unfounded: No evidence supporting allegation being made.
  - Unsubstantiated: Insufficient evidence to prove or disprove the allegation.

- 6.5 The Planning meeting should set a review date within one month of the referral being received with a view to concluding the enquiry as soon as possible.

## **7.0 DISCIPLINARY PROCEDURES**

- 7.1 Any disciplinary process must be clearly separated from child protection enquiries. There are three strands in the consideration of an allegation:
- A police investigation of a possible criminal offence
  - Social Care enquiries/assessment about whether a child is in need of protection or services
  - Consideration by an employer of disciplinary or capability action.
- 7.2 Insufficient evidence to support a Police investigation should not prevent any action being taken that is necessary to safeguard a child's welfare.
- 7.3 An allegation regarding inappropriate behaviour which is not considered sufficiently harmful under the child protection procedures may still need to be considered under the disciplinary procedures. If an allegation or concern arises about a member of staff, outside of their work with children, and this may present a risk of harm to children from which the member of staff is responsible for.
- 7.4 The Trust Designated Senior Manager should consult the Trust Disciplinary Procedures for guidance on suspension, referral to the DBS etc. If an allegation is substantiated and the staff member is dismissed or the employer ceases with the Trust consideration must be given to a referral to the Disclosure and Barring Service.

## **8.0 UNFOUNDED ALLEGATIONS**

- 8.1 If the allegation is determined to be unfounded the Trust Designated Senior Manager should consider:
- Referring the matter to Children's Social Care to determine if the child is in need or may have been abused by someone else;
  - Asking Police what action may be required in the rare event that the allegation was deliberately invented or malicious.
  - Support and Counselling services availability for staff via the Occupational Health Service.

## **9.0 SAFER WORKING PRACTICES FOR ADULTS WORKING WITH CHILDREN**

- 9.1 It is important that all staff working with children understand that the nature of their work and the responsibilities related to it, place them in a position of trust. Staff should note that:
- Staff who work with children are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.

- Staff should work and be seen to work, in an open and transparent way.
- The same professional standards should always be applied regardless of culture, disability, gender, language, racial origin, religious belief and/or sexual identity.

9.2 Staff whose practice deviates from this guidance and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people.

**9.3 Power and Positions of Trust**

As a result of their knowledge, position and/or the authority invested in their role, all adults working with children and young people are in positions of trust in relation to the young people in their care. A position of trust related to one in which one party is in a position of power or influence over the other by virtue of their work or the nature of their activity. It is vital for all Staff to understand the power this can give them over those they care for and the responsibility they must exercise as a consequence of this relationship.

9.4 A relationship between an adult and a child or young person cannot be a relationship between equals. There is potential for exploitation and harm of vulnerable young people. Adults have a responsibility to ensure that an unequal balance of power is not used for personal advantage or gratification.

9.5 Staff should always maintain appropriate professional boundaries and avoid behaviour which might be misinterpreted by others. They should report and record any incident with this potential. Where a person aged 18 or over is in a specified position of trust with a child under 18, it is an offence for that person to engage in sexual activity with or in the presence of that child, or to cause or incite that child to engage in or watch sexual activity.

**9.6 Communication with Children and Young People (*including Technology*)**

Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Staff should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Staff should ensure that all communications are transparent and open to scrutiny.

9.7 Staff should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between Staff and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.

Internal e-mail systems should only be used in accordance with Trust policy.

- 9.8 Any sexual activity between a member of staff and a child or young person, who is a service user, may be regarded as a criminal offence and will always be a matter for disciplinary action. Sexual activity referred to does not just involve physical contact including penetrative and non-penetrative acts. It may also include non-contact activities, such as causing children to engage in or watch sexual activity or the production of pornographic material.
- 9.9 There are occasions when adults embark on a course of behaviour known as 'grooming' where the sole purpose is to gain the trust of a child, and manipulate that relationship so sexual abuse can take place. Staff should be aware that consistently conferring inappropriate special attention and favour upon a child might be construed as being part of a 'grooming' process and as such will give rise to concerns about their behaviour.
- 9.10 It is recognised that some children who have experienced abuse may seek inappropriate physical contact. Staff should be particularly aware of this when it is known that a child has suffered previous abuse or neglect. In the child's view, physical contact might be associated with such experiences and lead to some actions being misinterpreted. In all circumstances where a child or young person initiates inappropriate physical contact, it is the responsibility of the staff member to sensitively deter the child and help them understand the importance of personal boundaries. Such circumstances must always be reported and discussed with a senior manager and the parent/carer.

**9.11 Intimate Care**

Some job responsibilities necessitate intimate physical contact with children on a regular basis, for example assisting young children with toileting, providing intimate care for children with disabilities or in the provision of medical care. The nature, circumstances and context of such contact should comply with professional codes of practice or guidance and/or be part of a formally agreed plan, which is regularly reviewed recorded and agreed by parents/ and child. The additional vulnerabilities that may arise from a physical or learning disability should be taken into account and be recorded as part of an agreed care plan. The emotional responses of any child to intimate care should be carefully and sensitively observed, and where necessary, any concerns passed to senior managers and/or parents/carers.

**9.12 Home Visits**

A risk assessment should include an evaluation of any known factors regarding the child/young person, parents and others living in the household. Risk factors such as hostility, child protection concerns, complaints or grievances can make adults more vulnerable to an allegation.

- 9.13 Staff should not visit a child in their home outside agreed work arrangements or invite a child to their own home or that of a family member, colleague or friend.

<b>END</b>
------------

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**PROCEDURE ON CHILD SAFEGUARDING PRACTICE REVIEWS**

**1.0 INTRODUCTION**

- 1.1 This procedure sets out the requirements for the Trust and staff to comply with *Working Together to Safeguard Children 2018*, and Local Safeguarding Children Partnership Procedural Guidance

The Safeguarding Partners, which are the Local Authority, Police and Clinical Commissioning Group, are responsible for instigating a Child Safeguarding Practice Review formally known as Serious Case Review (SCR).

- 1.2 The responsibility for how the system learns the lessons from serious child safeguarding incidents lies at a national level with the Child Safeguarding Practice Review Panel (the Panel) and at local level with the Safeguarding Partners. The Panel is responsible for identifying and overseeing the review of serious child safeguarding cases which, in its view, raise issues that are complex or of national importance. Locally, Safeguarding Partners must make arrangements to identify and review serious child safeguarding cases which, in their view, raise issues of importance in relation to their area.

- 1.3 Serious Child Safeguarding Cases are those where:

- Abuse or neglect of a child is known or suspected; AND
- The child has died or been seriously harmed and there is a concern on how partners have worked together to safeguard the child.
- Serious harm includes serious and/or long term impairment of a child's mental health or intellectual, emotional, social, physical or behavioral development. This definition is not exhaustive and even if a child recovers this does not mean serious harm cannot have occurred. Additionally serious harm includes a potentially life threatening injury.
- A child dies in custody or where the child was detained under the Mental Health Act.

- 1.4 The Local Authority must notify any event that meets the above criteria to the Panel within five working days of becoming aware that the incident has occurred. The Local Authority should also report the event to the Safeguarding Partners in their area within five working days. The duty to notify events to the Panel rests with the local authority and others who have functions relating to children should inform the Safeguarding Partners of any incident which they think should be considered for a child safeguarding practice review.

- 1.5 When considering the criteria for a child safeguarding practice review the Safeguarding Partners must take into consideration:

- highlights or may highlight improvements needed to safeguard and promote the welfare of children, including where those improvements have been previously identified

- highlights or may highlight recurrent themes in the safeguarding and promotion of the welfare of children
- highlights or may highlight concerns regarding two or more organisations or agencies working together effectively to safeguard and promote the welfare of children
- is one which the Child Safeguarding Practice Review Panel have considered and concluded a local review may be more appropriate
- where the safeguarding partners have cause for concern about the actions of a single agency
- where there has been no agency involvement and this gives the safeguarding partners cause for concern
- where more than one local authority, police area or clinical commissioning group is involved, including in cases where families have moved around
- where the case may raise issues relating to safeguarding or promoting the welfare of children in institutional settings

1.6 The Safeguarding Partners will undertake a rapid review of any new case that has been referred to them for consideration. This is then shared with the national panel and has a timescale of 15 days attached to it.

1.7 When the Trust is involved in a child safeguarding practice review a Serious Incident may also be carried out which is monitored by the Clinical Commissioning Group.

1.8 When the Safeguarding Partners decision has been made to undertake a local child safeguarding practice review a Trust Individual Management Review (IMR) or alternative review, e.g. a Multi-Agency Review (MAR) methodology will be agreed if the child or parent/carer is known or has been known to the Trust. The aim of the Individual Management Review or alternate Multi-Agency Review methodology is to look openly and critically at individual and organisational practice to identify:

- Areas of good practice;
- Whether the case indicates changes could and should be made;
- How these changes will be brought about and monitored.

1.9 The findings and analysis from the review will be brought together by an Overview Author commissioned by the Safeguarding Partners child safeguarding review Panel with other agencies/organisations into an 'Overview Report'. The Trust will be expected to implement specific recommendations by the LSCB, regardless of whether the Trust is directly involved in the case

## **2.0 PURPOSE OF CHILD SAFEGUARDING PRACTICE REVIEWS**

2.1 Establish whether there are lessons to be learned from a case about the way in which local professionals and agencies work together to safeguard children.

2.2 Identify clearly what those lessons are, how they will be acted upon and what is expected to change as a result.

- 2.3 Improve inter-agency working and better safeguard and promote the welfare of children.
- 2.4 Child Safeguarding Practice Reviews are not inquiries into how a child died or who is culpable. These matters are for Coroners and Criminal Courts respectively.
- 2.5 When there is a death or serious injury of a child and abuse or neglect are suspected to be factors in that death an assessment should be undertaken of whether there are other children in the household/family who require safeguarding. Where appropriate a referral should be made to social care regarding the remaining children in the family.

### **3.0 PROCESS**

- 3.1 Once it is known that a child/young person has died, or a case is being considered for a Child Safeguarding Practice Review the Head of Safeguarding will inform the Serious Incident Team (in order to reduce duplication of any parallel process) and the Executive Nurse.
- 3.2 The Trust Named Nurse/Practitioner Safeguarding will secure all relevant adult and child records.
- The records will be copied by the Safeguarding Team.
  - In the case of a child being taken into care the record should be forwarded on to the appropriate health professional where the child is residing.
- 3.3 The Designated Nurse for the relevant CCG should inform NHS Midlands and East and the Care Quality Commission of every case that becomes subject of a Child Safeguarding Review in their area.
- 3.4 The Trust Chief Executive will receive notification from the Child Safeguarding Partners of the Child Safeguarding Practice Review, and will be asked to nominate a Reviewing Officer to undertake the Individual Management Review (IMR). Reviewing officers will be supported by a member of the Safeguarding Team
- 3.5 Where a case involves a number of Trust services e.g. Community Health and Mental Health services, only one IMR will be required. Where it is deemed appropriate, separate IMR's may be agreed. The Reviewing Officer will co-ordinate the collection of records and liaise with other relevant Named Safeguarding Nurses/Practitioners as required.
- 3.6 The Reviewing Officer will review all case records on the child/children in order to:
- Complete a comprehensive, factual chronology of involvement by the professionals in contact with the child/children as set out in the Child Safeguarding Practice Review's terms of reference.
  - To compile a report which looks openly and critically at the involvement of professionals/services and contains analysis of the presenting facts?

- Develop a SMART action plan.
  - Identify any omissions in the Trust or LSCB Child Protection / Safeguarding Children Policies or Child Health Procedures.
- 3.7 The review report will be completed within the set timescales as stated in the terms of reference/scoping (usually one calendar month from the request).
- 3.8 Staff involved in the case may need to be interviewed by the Reviewing Officer using the LSCB interview format. A copy of the interview summary should be given to the interviewee.
- 3.9 The Reviewing Officer should ensure that appropriate support and supervision is offered to staff and interviewees.
- 3.10 The Individual Management Report will be submitted to the Trust Mental Health Act and Safeguarding Sub-Committee and Executive Team in order that it is ratified by the Trust Chief Executive.
- 3.11 The Head of Safeguarding will liaise with the Trust Communications department as necessary.
- 3.12 Any recommendations made in the IMR will be placed on the Trust Mental Health Act and Safeguarding Sub-Committee action plan and can be implemented as soon as possible. Any subsequent recommendations made from the overview report will also be placed on the action plan and monitored monthly for compliance.
- 3.13 Once the Individual Management Report has been submitted to the Child Safeguarding Practice Review Panel a feedback process and debriefing for staff involved should take place, which may be before the completion of the final report by the panel.
- 3.14 Where the Child Safeguarding Practice Review Panel commissions an alternative case review methodology, the Trust should co-operate to influence and agree the terms of reference.
- 3.15 Trust staff will be required to participate in appropriate learning events as part of the agreed commissioned case review and will be supported by their own operational managers and the Trust Safeguarding Named Nurse/Professionals.
- 3.16 A summary of the outcomes and recommendations of the final interagency Child Safeguarding Practice Overview Report will be presented to the Trust Mental Health Act and Safeguarding Sub-Committee and reported to the Executive Team as required.
- 3.17 Child Safeguarding Practice Reviews are not part of any disciplinary enquiry or process, but information that emerges from the Individual Management Review or alternative case review methodology could indicate that actions may be required, including disciplinary action.

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE**  
**APPENDIX 9**

- 3.18 The Full Overview Report compiled by the Child Safeguarding Practice Review Panel will be available to the public.
- 3.19 Implementation of Trust Action plans as part of the IMR or Overview report will be the responsibility of the Director of the Service/s involved in the case.
- 3.20 The implementation will be monitored via relevant service management, Community Services Safeguarding Children Groups and the Trust Mental Health Act and Safeguarding Sub-Committee.

<b>END</b>
------------

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**PROCEDURE FOR UNEXPECTED CHILD DEATH AND NATIONAL LEARNING  
DISABILITIES MORTALITY REVIEW PROCESSES**

**1.0 INTRODUCTION**

This procedure sets out the roles and responsibilities of Trust staff in responding to the death of a child and complies with *Working Together 2018* and the Local Safeguarding Partnership Procedures for responding to deaths in childhood. This Procedure outlines staff roles in responding to the death of a child and should be read in conjunction with the local area Safeguarding procedures.

- 1.1 Child Death Review Partners are required to be notified of the death of any child 0- 18 years whether from natural, unnatural, known or unknown causes, at home, in hospital or in the community
- 1.2 It is important to specifically recognise and record if a child or young person has learning disabilities, irrespective of any other diagnoses or syndromes that are recognised. The Learning Disabilities Mortality Review (LeDeR) programme describes a review process for the deaths of people aged 4 years and over with Learning Disabilities in England.
- 1.3 There are two inter-related processes for reviewing child deaths. Either process can trigger a Child Practice Safeguarding Review formally known as a Serious Case Review (SCR). The processes are:
  - Rapid response by a group of key professionals coming together for the purpose of enquiring into and evaluating each unexpected death of a child;  
and
  - An overview of all child deaths up to the age of 18 years (excluding both those babies who are stillborn and planned terminations of pregnancy carried out within the law) in the Local Safeguarding Partnership area/s, undertaken by a panel.

**2.0 PURPOSE**

- 2.1 The purpose of the procedure for unexpected child death review is to collect and analyse information about all local childhood deaths with a view to identifying:
  - Cases requiring serious case review.
  - Concerns affecting the safety and welfare of children.
  - Wider public health or safety concerns arising from a particular death or from a pattern of deaths.
  - A coordinated agency response to all unexpected deaths of children.

- 2.2 There is a process to be followed when responding to, investigating, and reviewing the death of any child, from any cause. This is for two main reasons:
- to improve the experience of bereaved families, as well as professionals, after the death of a child; and
  - to ensure that information from the child death review process is systematically captured to enable local learning and, through the planned National Child Mortality Database, to identify learning at the national level, and inform changes in policy and practice
- 2.3 Minorities of unexpected deaths are the consequence of abuse or neglect, or are found to have abuse or neglect as an associated factor. In all cases, enquiries should seek to understand the reasons for the child's death and also consider any lessons to be learnt about how best to safeguard and promote children's welfare in the future.
- 2.4 The purpose of the local reviews of deaths of a child with learning disabilities is to identify any potentially avoidable factors that may have contributed to the person's death and to develop plans of action that individually or in combination will guide necessary changes in health and social care services in order to reduce premature deaths of people with learning disabilities.
- 2.5 Child suicide should be reviewed in the same manner as other child deaths, with the following expectations:
- Deaths related to suspected suicide and self-harm should be referred to the coroner for investigation;
  - Deaths related to suspected suicide and self-harm will require a Joint Agency Response;
  - The Child Death Review Meeting should include experts in mental health and key professionals involved in the child's life across education, social services and health.
- 2.6 All child deaths in an inpatient mental health setting (general and secure) whether they are treated 'voluntarily' as informal inpatients or detained under the Mental Health Act 1983 (MHA) will be subject to the child death review process and reported to the coroner. When a child dies while detained under the MHA, there should also be a Child Safeguarding Practice Review. The Child Death Review Meeting should involve the care coordinator for the community mental health team as well as other professionals from children and young people's mental health services.
- 2.7 An unexpected death of a child will be subject to an investigative process by the Rapid Response Team which is made up of a;
- Consultant Paediatrician (responsible for ensuring the process is correctly carried out).
  - Police officer.
  - On call health professional.
  - Children's social worker if there has been prior involvement or abuse or neglect is suspected to be a factor in the death.

2.8 This procedure will primarily apply to staff working directly with children and young people and on call managers. However there may be occasions where information on a parent is required from adult services. Therefore all staff working with children and adults should be aware of this procedure which outlines roles and responsibilities in responding to the death of a child or young person and consideration of the possible needs of other children in the household and other family members.

<b>3.0 DEFINITION</b>
-----------------------

3.1 An 'unexpected death' of a child occurs where;

- Death was not anticipated as a significant possibility 24 hours before it occurred
- or
- There was a similarly unexpected collapse leading to or precipitating the events which led to the death.

3.2 A Designated paediatrician will be notified of **all** unexpected deaths in childhood. When staff are uncertain about whether the death is unexpected the Designated Paediatrician should be contacted.

3.3 Each area may have a Local Child Death Review Panel (LCDRP) whose functions are to collect and analyse information relating to the death of any child in their area. The panel will identify any matters of concern giving rise to the safety and welfare of children in their area along with any wider public health or safety concerns.

3.4 A Child Death Overview Panel (CDOP) will be responsible for reviewing information on all child deaths in order to enable the Local Safeguarding Partnership to carry out its statutory functions relating to child deaths. The CDOP Panel has a permanent core membership drawn from the key organisations represented on the Local Safeguarding Partnership. Trust Community Health staff may become members of a CDR and should refer to specific Local Safeguarding area guidance.

3.5 The Learning Disabilities Mortality Review (LeDeR) programme defines 'learning disabilities' to include the following:

- Significantly reduced ability to understand new or complex information and to learn new skills (impaired intelligence), with
- Reduced ability to cope independently (impaired social functioning), which
- Started in childhood with a lasting effect on development.

3.6 The child death review process will be the primary review process for children with learning disability and it will not be necessary for the LeDeR programme to review each case separately. When notified of the death of a child or young person aged 4-17 years who has learning disabilities, or is very likely to have learning disabilities but not yet had a formal assessment for this, the local CDR Partners should report that death to the LeDeR programme

## 4.0 PROCESS

- 4.1 Death should not be assumed and if a child appears to have died or collapses, an ambulance should be called and resuscitation attempted until the arrival of the ambulance.
- 4.2 A child should be immediately transferred to A&E where the designated paediatrician declaring the death or clinical specialist for child death will be responsible for initiating the rapid response (if the death is unexpected) / child death review process.
- 4.3 The Rapid Response Team will be identified within 4 hours of the death being notified.  
The Rapid Response Team will decide on action to be taken for example:
- Visit to scene of death (within 24hrs and prior to post mortem).
  - Notification to relevant professionals.
  - Obtaining information from relevant professionals.
- 4.4 If declared dead at the scene the health professional is responsible for identifying anything about the child's death which gives rise for concern or cause for suspicion and for passing these concerns on to the appropriate authority. The professional is also responsible for initiating the rapid response / child death review process by notifying the death in the usual way using the **Notification Form**. It is the responsibility of the General Practitioner (GP) or health professional present to record information about the sense of death that would normally have been collected via this process and to make this available to child death panel manager/administrator.
- 4.5 Trust staff may be contacted by other NHS professionals to identify if a child has been known to Trust services. Staff should co-operate with sharing information.
- 4.6 If a death is identified as suspicious the Police are the lead investigating agency. If criminal proceedings are necessary the Child Death Review Process will cease until notified otherwise by police.
- 4.7 Trust Staff should inform the Trust Safeguarding Team and record all information as soon as possible in the child/Young person's records. Trust Incident Forms should be completed as per Trust policy.
- 4.8 Trust staff directly involved with a case will be expected to complete a copy of the data set or a written report for the child Death Review Team within ten working days using the **Reporting form B** and the relevant **sub B. Forms** will be sent to staff from the Child Death Review Administrator.
- 4.9 All staff that have had contact with a child who has died will be asked to share information on the child for the purposes of informing the professional response and work of the Child Death Review Panels.
- 4.10 Where a health care practitioner becomes aware of a death, they should check that the relevant Child Health Information Department have been notified.

- 4.11 Records should be retained for all child deaths until discussion of the case at the child death review panel and then stored in accordance to Trust record keeping and storage policy.
- 4.12 Copies of all forms and reports should be sent to the Trust Safeguarding Team.
- 4.13 The Child Death Review Team will continue to meet to discuss the case and identify findings or additional input required by professionals.
- 4.14 A visit to the scene of the death will be undertaken by the Police Officer and Clinical Specialist for Child Death forming the rapid response team. A health visitor, GP or other similar professional who has had previous contact with the family may also participate in the home visit to provide support.
- 4.15 Ongoing bereavement support for the family may be identified by Community Healthcare and CAMHS teams who may be asked to offer services to siblings where appropriate.
- 4.16 If concerns are raised at any stage about the possibility of surviving children in the household being abused or neglected, the Trust Safeguarding policies & procedures should be followed and Children's Social Care notified.
- 4.17 Where a case is transferred for a Local Safeguarding Child Practice Review formally known as Serious Case Review Panel the Trust will comply with the Child Safeguarding Practice Review procedures and complete an Individual Management Review where required. This may be in addition to an internal Serious Incident Investigations which may be required.

## **5.0 LESSONS LEARNED**

- 5.1 The Child Death Review Partners will aggregate the findings from all child deaths, collected according to a nationally agreed minimum data set, to inform local strategic planning on how best to safeguard and promote the welfare of the children in the local authority area.
- 5.2 The Child Death Review Partners are responsible for disseminating lessons in order to improve policy, professional practice and interagency working.
- 5.3 All relevant recommendations will be placed on the Trust Mental Health Act and Safeguarding Sub-Committee action plan.
- 5.4 Where appropriate cases will be placed on the 'Lessons Learned' section of the Trust Safeguarding link on the Intranet.

**END**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**PROCEDURE FOR COURT APPEARANCE & FORMAL STATEMENTS**

**ASSURANCE STATEMENT**

This procedure sets out the roles and responsibilities of Trust staff in responding to requests for statements and appearance at Court Proceedings.

**1.0 Requests for formal statements and information**

**1.1 Introduction**

- 1.1.1 Staff are required to co-operate with police and the Local Authority when approached for a formal statement. In these circumstances staff must inform the relevant Safeguarding Team and their line manager. The Trust Legal Advisor can be contacted for advice and support.
- 1.1.2 Any requests for information relating to Legal Safeguarding Processes should be made in writing with an explanation as to the jurisdiction the information is being requested and should include the Access to Records team.

**1.2 Statements for police**

- 1.2.1 These are usually requested by the police working within the Public Protection units when a criminal offence against a child/young person is suspected or has been committed.
- 1.2.2 In the event of the Police Officer directly requesting an interview/witness statement the member of staff must inform the Line Manager and a member of the Safeguarding Team immediately.
- 1.2.3 Arrangements can be made for the member of staff to meet with the Police, accompanied by a member of the Safeguarding Team or line manager.
- 1.2.4 The member of staff must have the relevant child's/children's records with them to refer to.
- 1.2.5 Statements must be based on facts, your observations and actions, with the distinction made between facts, opinions, observations and hearsay.
- 1.2.6 Professional opinions may be requested and must be substantiated and recorded as such.
- 1.2.7 Staff should ensure they read their statement carefully before signing and amend any points in the statement that they feel do not accurately reflect responses to the Police Officer's questions before signing.

- 1.2.8 Members of staff will not receive a copy of this statement for reference; however you will receive paperwork acknowledging giving of the statement. A record should be made in the appropriate child health record that a police statement has been given and who was present.

### **1.3 Local Authority Solicitor**

- 1.3.1 The Local Authority Solicitor will send a formal request to the Safeguarding Team/Access to Records team usually accompanied by a copy of the Court Directions, if appropriate.
- 1.3.2 The Safeguarding Team will support staff in the preparation for Court Statements using the appropriate local template.
- 1.3.3 A copy of the typed and signed statement will be retained by the Safeguarding Team, Access to records team and the member of staff making the statement.

### **1.4 Private Solicitors**

- 1.4.1 There will certainly be occasions when community professionals are requested to write letters to the Court in support of access requests, or to give evidence of the impact of parental separation and divorce on the child/children on behalf of either parent.
- 1.4.2 Any statement given by a professional worker could be constructed by other parties involved as evidence of favour. For this reason, staff must not give any information, which may be used in legal situations, unless directed by the Court. This is to protect both clients and professionals in order that no party is given favour, or preferential treatment.
- 1.4.3 No statement on safeguarding children matters should be given without advice and support from the Safeguarding Team/Access to Records team who will seek further advice as appropriate.
- 1.4.4 The member of staff's line manager should be made aware of all requests.

### **1.5 Children and Family Court Advisory Service (CAFCASS) and Children's Guardian**

- 1.5.1 Requests for information must be in writing. No information to be given on the telephone.
- 1.5.2 Arrangements must be made with the Safeguarding Team for cases that relate to safeguarding children to prepare a report or to jointly meet with the CAFCASS Officer and the Children's Guardian where necessary.

### **1.6 Social Worker**

- 1.6.1 Occasionally a Social Worker will request information that is related to safeguarding children legal matters. The Social Worker will be informed that this request must be made in writing to the Named Nurse/Doctor Safeguarding Children who will then advise the professional on what action

needs to be taken.

- 1.6.2 Arrangements will be made with the Safeguarding Team and the member of staff to prepare a report.

## **2.0 Preparation for Court Statement**

2.1.1 All statements can be prepared with the support of the Trust's Safeguarding Team and will be based on information contained in the professional records.

2.1.2 The statement will include:

- The professional's details:
  - Full name
  - work address
  - occupation and qualifications.

- The extent of the professional's involvement with the family.
- Contacts with the child/family including no access.
- Growth and development of the child.
- Relationships within the family and the effect they have had on the child.
- Significant events that may have affected the child.
- A professional opinion on whether the health needs of the child is being met.
- The concerns that the professional has and whether these have been referred to another agency.
- Conclusion and recommendation.
- Full signature and date.
- Legal advice and information regarding giving evidence on your statement may be made available if necessary, from Trust Solicitor.
- Copies of statements must be retained.
- Line Managers and the Access to Records team must be made aware of all requests for statements and court appearances.

## **2.2 Attendance at Court**

2.2.1 A member of staff may be advised well in advance of the dates of a pending Court Case (criminal proceedings) and these should be diarised immediately. The manager and Safeguarding Team must be informed.

2.2.2 If a member of staff is required to give evidence in Court regarding Local Authority applications, arrangements will be made by the Local Authority's Solicitor's department in agreement with the Safeguarding Team.

2.2.3 Some orders may require a subpoena but the majority of Local Authority Court actions will be conducted with the full co-operation of health care staff.

- 2.2.4 There are two types of proceedings:
- Care Proceedings – taken by Social Care to protect the welfare of the child.
  - Criminal Proceedings – taken by Police when an alleged abuser is charged with an offence of abuse.
- 2.2.5 The Safeguarding Team will advise on what to expect in Court proceedings and presentation of evidence.
- 2.2.6 The Trust legal advisor may be asked to advise on presentation of evidence
- 2.2.7 The staff member will ensure that all records relating to the child and relevant adults are taken to Court and are available for easy access in line with Information Governance requirements, if required.
- 2.2.8 A member of the Safeguarding Team or Line Manager will accompany the member of staff to Court where applicable.
- 2.2.9 The Line Manager will ensure that the staff member is provided with sufficient time and support to undertake this responsibility.

<b>3.0 Guidance on Court Appearance as a Witness</b>
--

- 3.1 The Safeguarding Team will support staff in the preparation for witness appearance in Court
- 3.2 Members of staff may be called to give evidence in either or both Care Proceedings or Criminal Proceedings. (A child witness may give evidence via a video link).
- 3.3 On arrival at the Court, witnesses must make themselves known to the Clerk to the Court and ascertain in which Court the Hearing will be held.
- 3.4 Security screening operates in the Courts.
- 3.5 In Care Proceedings, the Local Authority Solicitor will question staff witness initially, followed by the Solicitors for the other parties.
- 3.6 An opinion may be sought and a staff acting as witness can only comment on issues within their field of expertise.
- 3.7 In the event of the Hearing being reconvened, the Reports may need to be updated.
- 3.8 The Line Manager will ensure that the staff member is provided with sufficient time and support to undertake this responsibility.
- 3.9 The member of staff should be offered the opportunity for a formal debrief, by either line manager or member of the Trust Safeguarding Team.

<b>END</b>
------------

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROCEDURE FOR PREVENT

Assurance Statement

This procedure sets out the requirements for the Trust staff who work with service users where there are concerns regarding terrorism and complies with the Home Office Prevent strategy 2011 'Building Partnerships staying safe'. Contest is overall UK strategy for counter terrorism and was updated in June 2018.

**1.0 Introduction**

- 1.1 This procedural guidance is relevant for all staff working with child adults and older people.
- 1.2 CONTEST is the Government's national counter terrorism strategy, aims to reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence.

The strategy has four work streams as below and it is the Prevent work stream that is relevant for NHS staff:

- Pursue: to stop terrorist attacks in the UK and overseas
- Protect: to strengthen our protection against terrorist attack
- Prepare: where an attack cannot be stopped, to mitigate its impact
- **Prevent: safeguard people from becoming terrorists or supporting terrorism**

- 1.3 Prevent aims to stop people from becoming terrorists or supporting terrorism. The Department of Health (DH) have worked with the Home Office to develop guidance for healthcare organisations to implement Prevent locally, called "Building Partnerships Staying Safe". The aim is to re-enforce safeguarding at the heart of Prevent to ensure our communities and families are not exploited or groomed into following a path of violent extremism

The Prevent Strategy addresses all forms of terrorism including extreme right wing but continues to prioritise according to the threat posed to our national security. The aim of Prevent is to stop people from becoming terrorists or supporting terrorism and operates in the pre-criminal space before any criminal activity has taken place.

- 1.4 The three key objectives of the Prevent Strategy are to:
  - Tackle the causes of radicalisation and respond to the ideological challenge of terrorism.
  - Safeguard and support those most at risk of radicalisation through early intervention, identifying them and offering support.
  - Enable those who have already engaged in terrorism to disengage and rehabilitate

Trust staff are expected to be involved in delivering objectives 2 and 3 only.

## **2.0 NHS engagement with the Prevent Strategy**

2.1 The Department of Health is a key strategic partner in The Prevent Strategy as Healthcare professionals may meet and treat people who are vulnerable to radicalisation. People with mental health issues or learning disability may be more easily drawn into terrorism. People connected to the healthcare sector have taken part in terrorist acts in the past.

## **3.0 Supportive documents**

3.1 This protocol should be used alongside Trust

- Serious Untoward Incidents
- Whistle blowing
- Local Safeguarding Prevent Policies and Procedures

3.2 National Guidance

- General Data Protection Regulations 2018.
- Human Rights Act 1998.
- Terrorist Act 2006.
- Equality Act 2010.
- Care Act 2014.
- Working Together to Safeguard Children 2018.

## **4.0 Definition of terms**

4.1 **Terrorism** is defined in the Terrorism Act of 2000 (TACT 2000) as an action that endangers or causes serious violence to a person or people, causes serious damage to property or seriously interferes or disrupts an electronic system. The use of threat must be designed to influence the government or to intimidate the public and is made for the purpose of political, religious or ideological gain.

4.2 **Radicalisation** is defined as the process by which people come to support terrorism and extremism and, in some cases, to then participate on terrorist activity.

4.3 **Extremism** is vocal or active opposition to fundamental values including democracy, the rule of the law, individual liberty, and mutual respect and tolerance of different beliefs and faiths. We also include in our definition of extremism, calls for the death of members of our armed forces, whether in this country or overseas.

4.4 A Prevent Concern does not have to be proven beyond reasonable doubt; however, it should be based on something that raises concern which is assessed by using existing professional judgement of a health or social care member of staff.

- 4.5 **Vulnerability** in the context of Prevent is a person who is **susceptible** to extremists' messages and is at risk of being drawn into terrorism or supporting terrorism at a point in time.

## **5.0 The Role of the Trust in delivering the Prevent Strategy**

- 5.1 The Trust has a duty to ensure safe environments where extremists are unable to operate. It is essential, therefore, that all staff know how they can support vulnerable individuals (patients or members of staff) who they feel may be at risk of becoming a terrorist or supporting extremism.

- 5.2 It should be stressed that there is no expectation that the Trust will take on a surveillance or enforcement role as a result of Prevent. Rather, it must work with partner organisations to contribute to the prevention of terrorism by safeguarding and protecting individuals and making safety a shared endeavour. In order to achieve this, the Trust has:

- Identified a PREVENT Lead – who is the Clinical Specialist for Safeguarding
- Appropriate staff to provide and deliver the Workshop to Raise Awareness of Prevent (WRAP) training to key frontline staff and ensure Prevent awareness is available through the mandatory Safeguarding Children and Adults Training at Level 1-3
- Ensure staff know how to escalate any concerns relating to a service user or colleague's wellbeing and/or the safety of the public
- Promoted the responsible and effective use of the internet by all staff, volunteers and patients
- Build and strengthen local partnership and inter-agency working to prevent vulnerable individuals from becoming the victims or causes of harm.

### **5.3 Training requirements**

- 5.3.1 Awareness of Prevent issues is incorporated into Safeguarding Level 1-3 training programmes for children and adults.

- 5.3.2 In addition specific staff are required to complete an OLM E-learning package called Workshop to Raise Awareness of Prevent (WRAP) training.

- 5.3.3 All required staff will have this training placed onto the training tracker system and compliance reported monthly at the Safeguarding meeting.

- 5.3.4 The Trust will provide reports on training and Prevent activity to the CCG and Local Safeguarding Boards

## **6.0 Assessing Vulnerability**

### **6.1 Identifying Vulnerable People**

There are a number of behaviours and other indicators that may indicate that an individual is engaged with an extremist group, cause or ideology. The examples below are not exhaustive and vulnerability may manifest itself in other ways.

There is no single route to terrorism nor is there a simple profile of those who become involved. For this reason, it must not be assumed that these characteristics and experiences will necessarily lead to individuals becoming terrorists.

- Spending increasing time in the company of other suspected extremists;
- Changing their style of dress or personal appearance to accord with the group;
- Their day-to-day behaviour becoming increasingly centred around an extremist ideology, group or cause;
- Loss of interest in other friends and activities not associated with the extremist ideology, group or cause;
- Possession of material or symbols associated with an extremist cause (e.g. The swastika for far right groups);
- Attempts to recruit others to the group/cause/ideology.
- Communications with others that suggest identification with a group/cause/ideology.

## **7.0 Reporting a Prevent concern**

7.1 Where staff are concerned or suspect that a service user or colleague is involved in Prevent activity or express radical extremist views or vulnerable to grooming or exploitation by others, the usual safeguarding procedure should take place and a discussion with a member of the Safeguarding team is advisable.

### **7.2 Consent**

7.2.1 People who are vulnerable to violent extremism or radicalisation are more likely to be reached by supportive services if issues of consent are handled with sensitivity and an informed understanding of the issues. Before making a referral, staff should clarify the information.

7.2.2 For children this will ordinarily involve talking to the child/young person and their family (unless the family is implicated in potential extremism), and to other professionals working with the child/young person. Any referral should be made with the young person/family's knowledge and consent, unless to do so would place the child/young person at risk of harm.

7.2.3 For adults (over 18 years old) practitioners should seek the consent of the person who may be at risk of extremism or radicalisation before taking action or sharing information. In some cases, where a person refuses consent, information can still lawfully be shared if it is in the public interest to do so. This may include protecting someone from serious harm or preventing crime and disorder.

When there are grounds to doubt the capacity of those aged 16 then a capacity assessment should be considered in line with the Mental Capacity Act 2005 in order to support the person being able to give informed consent

7.2.4 Any practitioner who is in doubt about whether or not they should share information, or whether they have consent either to share information or carry out a piece of work, should consult with their line manager, safeguarding team or Prevent Lead.

### **7.3 What to do if concerned see appendix 1 flow chart**

7.3.1 Where staff are concerned or suspect that a service user or colleague is involved in Prevent activity or express radical extremist views or vulnerable to grooming or exploitation by others, the usual safeguarding procedure should take place.

- A DATIX should be raised
- The safeguarding team contacted.
- A safeguarding children, adult and or Prevent referral form should be completed. This is known as a person vulnerable to radicalisation (VTR) form.

7.3.2 Where it is felt there is imminent risk of harm staff should ring Police on 999.

7.3.3 If staff are contacted by police enquiring about a service user or individual regarding Prevent activity then they must ask police to contact the Trust Prevent Lead or member of the safeguarding team.

7.3.4 The Safeguarding Team will work with police and other relevant professionals to convene a strategy meeting to determine:

- a) if the concerns presented constitute a Prevent Referral
- b) By sharing the information, the intention is to protect the individual from criminal exploitation, grooming (being drawn into terrorism) or self harm?
- c) In sharing information, is a serious crime being prevented or detected?
- d) In being drawn into terrorism does this individual pose harm to themselves or the wider public?
- e) The Safeguarding Team will consult with the Trust Caldicott Guardian in determining whether to breach confidentiality in the Public Interest under the General Data Protection Regulations.
- f) Where the Prevent Concern is in respect of a staff member, the Trust Director of Workforce and the Area Operational Director will be invited to attend the strategy meeting. Referral to Occupational Health or involvement of Occupational Health at the strategy meeting may also be considered. **The final decision to share information about a member of staff with police remains with the Trust Executive Medical Director.**

## **8.0 Channel Panels**

8.1 Channel Panels oversee and co-ordinate Prevent referrals and interventions. Channel is a process for providing support to people at risk that are being drawn into terrorism as a result of their vulnerability. The panel has a statutory basis: under the terms of the Counter Terrorism and Security Act 2015, and each local authority will have a Panel to:

- Explore the case and risks.
- Develop a support plan for accepted cases and signpost to other support where cases are not accepted.
- Ensure consent is sought prior to support being provided.
- Co-operate with other panel partners.

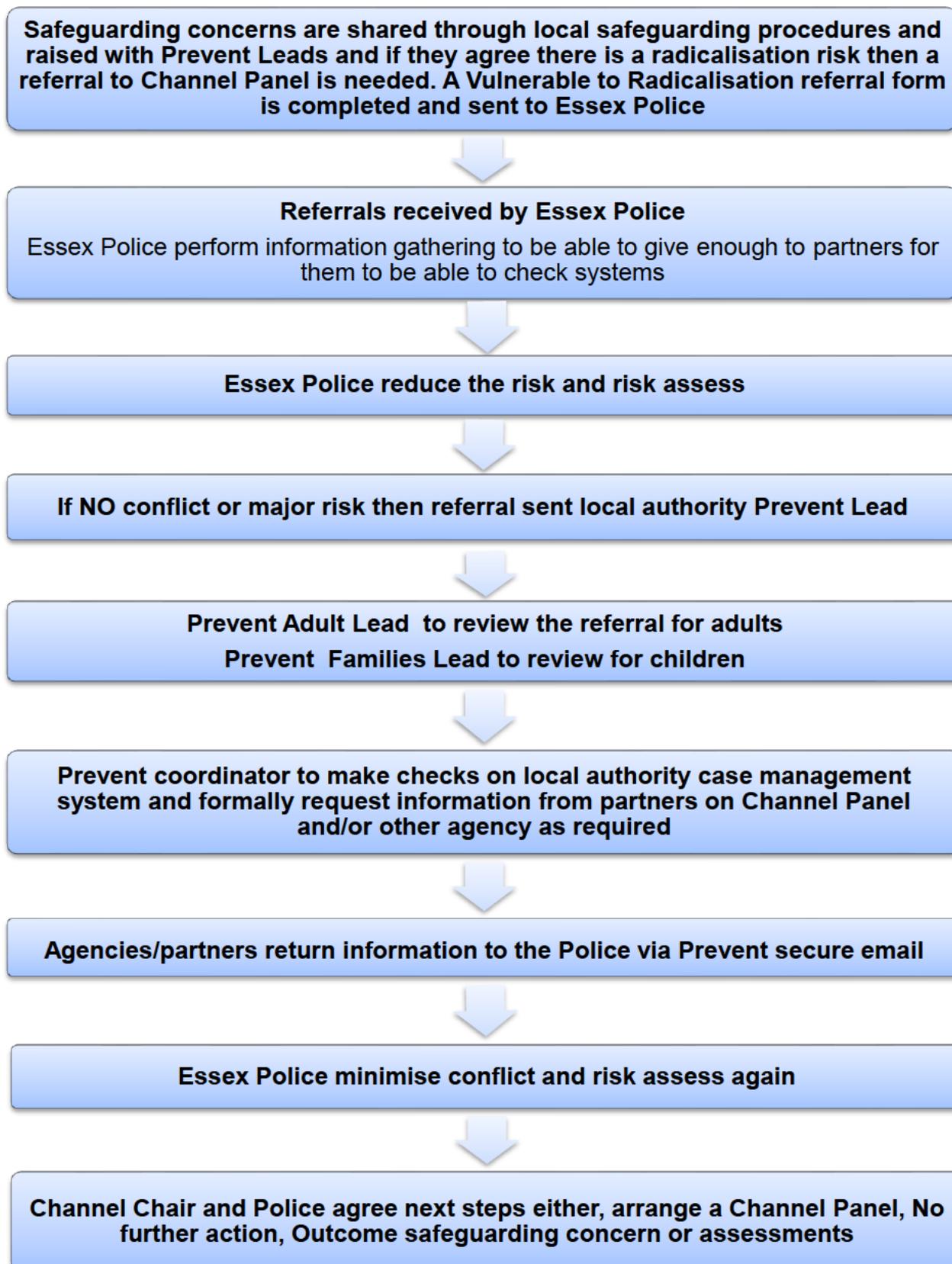
8.2 A member of the Trust Safeguarding team will attend the panel where appropriate. The Key worker for the child and or adult may also be invited. Channel assesses vulnerability by reviewing a vulnerability assessment framework with three dimensions:

- Engagement with a group, cause or ideology
- Intent to cause harm
- Capability to cause harm

**CLPG37 - SAFEGUARDING CHILDREN PROCEDURE  
APPENDIX 11**

- 8.3 If the panel is satisfied that the risk has been successfully reduced or managed they should recommend that the case exits the process.
- 8.4 If the panel is not satisfied that the risk has been reduced or managed the case is reconsidered. A new support plan should be developed and alternative support put in place. If the risk of criminality relating to terrorism has increased the Police Prevent team must consider escalating the case through existing police mechanisms.
- 8.5 The minutes of Prevent meetings will be stored securely by the Safeguarding Team and if appropriate will be included in either the service user's clinical records or the relevant electronic staff record.

Appendix 1 Referral Flow Chart



## INFORMATION GOVERNANCE AND SECURITY POLICY

<b>POLICY REFERENCE NUMBER:</b>	CP50
<b>VERSION NUMBER:</b>	3
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	3 year review
<b>AUTHOR:</b>	<div style="background-color: black; width: 100px; height: 15px; margin-bottom: 5px;"></div> Information Governance Manager
<b>CONSULTATION GROUPS:</b>	Information Governance Steering Sub-Committee. Quality Committee.
<b>IMPLEMENTATION DATE</b>	May 2018
<b>AMENDMENT DATE(S)</b>	Feb 2018; May 18 (GDPR); May 2021
<b>LAST REVIEW DATE</b>	May 2021
<b>NEXT REVIEW DATE</b>	May 2024
<b>APPROVAL BY IGSSC</b>	April 2021
<b>RATIFIED BY QUALITY COMMITTEE</b>	May 2021
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2018-2021. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

PROCEDURE SUMMARY		
<p>The purpose of this procedural guideline is to establish the governance arrangements and responsibilities for information security, with the intention to promote and build a level of consistency across the Essex Partnership University NHS Foundation Trust ('the Trust') to safeguard information, ensuring all Trust staff are aware of their individual responsibilities.</p>		
<p><b>The Trust monitors the implementation of and compliance with this procedure in the following ways:</b></p>		
<p>The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate. Also through Trust Datix Reporting and Compliance with the IG Data Security &amp; Protection Toolkit submission</p>		
Services	Applicable	Comments
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is**  
**The Executive Chief Finance & Resources Officer**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**INFORMATION GOVERNANCE AND SECURITY POLICY**

**CONTENTS**

- 1.0 INTRODUCTION**
- 2.0 DUTIES**
- 3.0 DEFINITIONS**
- 4.0 PRINCIPLES**
- 5.0 MONITORING OF IMPLEMENTATION & COMPLIANCE**
- 6.0 SCOPE OF POLICY**
- 7.0 MONITORING, REVIEW & PERFORMANCE MANAGEMENT**
- 8.0 ABUSE OF TRUST FACILITIES**
- 9.0 TRAINING**
- 10.0 REFERENCE TO OTHER TRUST POLICES / PROCEDURES**

SAMPLE ONLY

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST****Information Governance and Security Policy****1.0 INTRODUCTION**

- 1.1 The information used by the Trust is a vital business asset in terms of both clinical management of patients and the efficient management of services and resources. Protecting its confidentiality, integrity and availability is essential in preserving the Trust's reputation, efficiency, and its ability to comply with legal obligations.
- 1.2 Information / data has a key role in clinical and corporate governance, service planning and performance management.
- 1.3 Information governance deals with the way an NHS Trust handles personal, confidential and sensitive information / data about patients and staff and allows organisation and individuals to ensure that such information is dealt with in line with legislation, securely, efficiently and effectively.
- 1.4 Information governance will form the framework that merges all of the standards and best practice that apply to handling of person identifiable information / data.
- 1.5 It is vital therefore, that information / data is efficiently managed and that the appropriate policies and procedures are in place with management accountability and structures to provide a robust governance framework for information / data management.
- 1.6 To function effectively, ethically and legally the Trust needs to work within a framework of agreed rules.
- 1.7 This document sets out the Trust's intent for the safe and legal use of the facilities / systems provided by the Trust.
- 1.8 This policy and its associated procedures should be read in conjunction with other national guidance, Trust policies and other relevant legislation, including:
- Information Quality Assurance
  - British Standard for Information Security ISO/IEC27000 series
  - NHS Caldicott Report Recommendations
  - The National Health Service Act (2006)
  - Data Protection Act (2018)
  - General Data Protection Regulation
  - Access to Health Records Act (1990) (Where not superseded by the Data Protection Act (2018))
  - Freedom of Information Act (2000) (FOI) (including Publication Scheme)
  - The Environmental Information Regulations (2004) (EIR)
  - Computer Misuse Act (1990)

- Electronic Communications Act (2000)
- The Re-Use of Public Sector Information Regulations (2005)
- The Civil Contingencies Act (2004)
- The Human Rights Act (2000)
- The Copyright, Designs and Patents Act (1988) (as amended by the Copyright Computer Programs Regulations (1992))
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Crime and Disorder Act (1998)
- Health and Social Care Act (2000)
- The Common Law Duty of Confidentiality
- Integrated Governance Strategy
- Information Governance Framework
- Records Strategy
- IM&T Security Policy
- Data Protection and Confidentiality Policy / Procedure
- Freedom of Information Policy / Procedure
- Records Management Policy and related Procedures
- Mobile Working and Remote Access Policy/Procedures
- Data Quality Policy
- Virtual Private Network Policy
- Closed Circuit Television (CCTV) Policy / Procedure
- Information Governance and Security Procedures
- Paper and Electronic Corporate Records (Laserfiche) Policy / Procedures
- IT&T Security Procedures
- Internet/Email Access and Use Procedures
- Information Sharing & Consent Policy / Procedure
- ***This list is not exhaustive...***

- 1.9 There are many different types of legislation which relate to Information Governance, some are listed above but there is a full list in the Department of Health NHS Information Governance Guidance to Legal and Professional obligations

## 2.0 DUTIES / RESPONSIBILITIES

- 2.1 For the purposes of this policy, the definition of all staff includes all personnel working for or with the Trust, or who have been authorised to access the Trust's information assets. This includes all management, permanent employees, contractors, temporary staff, bank staff, locum, consultants, and agents/agency employees (***this list is not exhaustive***).
- 2.2 All employees of the Trust, permanent employees, contractors, temporary staff, bank staff, locum, consultants, and agents/agency employees (***this list is not exhaustive***) are required to abide by the contents of this policy and its associated procedural guidelines. Failure to do so may result in disciplinary action.

## **Responsible Persons**

### **2.3 Overall Responsibility Chief Executive**

- 2.3.1 The Chief Executive has overall responsibility as accountable officer for the management and implementation of information governance / security for the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.
- 2.3.2 As such the Chief Executive Officer signs up to the 'Statement of Compliance' declaration agreeing with its strict terms and conditions in relation to the security requirements for using N3 and for access to the Internet and NHS Connecting for Health applications.

### **2.4 Senior Information Risk Owner (SIRO).**

- 2.4.1 The Chief Executive has delegated the day to day responsibility for information governance / security, policy and implementation to the Executive Chief Finance Officer as the Trust's Senior Information Risk Owner (SIRO).
- 2.4.2 Making arrangements for information governance / security by setting / agreeing the overall policy for the Trust taking into account legal and NHS requirements.
- Appointing the Information Governance Security Manager / key leads.
  - Appointing a Data Protection Officer to ensure that the provision of the Data Protection Act / GDPR is satisfied.
  - Ensuring that, where appropriate, staff receive information governance / security awareness and training
  - Chairing the Information Governance Steering Sub-Committee on a regular basis and through the Committee maintaining the Trust's Information Governance / Security risk register and escalating any related risks to the Quality Committee

### **2.5 Caldicott Guardian**

- 2.5.1 The Chief Executive has delegated responsibility for Caldicott issues to the Executive Medical Director, who is the Caldicott Guardian. The Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of their person identifiable information / data, together with ensuring that patient identifiable information / data is shared in an appropriate and secure manner.

2.5.2 The Trust has dedicated forums for the monitoring of Caldicott Principles through the:

- Clinical Governance & Quality Committee
- Information Governance Steering Sub-Committee
- Caldicott Network

who are responsible for:

- Developing local protocols governing the disclosure of patient information to other organisations.
- Performing regular reviews and justifying the uses of patient information.
- Establishing access control policies for patient identifiable information.
- Improving organisational performance.
- Approving major initiative to enhance information governance / security.
- Reviewing and monitoring security incidents and compliance to this policy and its associated procedures.
- Monitoring significant changes in the exposure of information assets to major threats.

## 2.6 Information Governance Manager

2.6.1 The Information Governance Manager and / or Information Governance Administrators will oversee the day to day information governance issues and is responsible for:

- Working closely with the Trust's key information governance / security leads to ensure the actions below are implemented:
- Acting as a central point of contact on information governance / security within the Trust, for both staff and external organisations.
- Co-ordinating all Information Governance initiatives and producing the annual improvement plan / work programme
- Providing operational support for legal requirements, e.g. General Data Protection Regulation Data Protection Act (2018) and Freedom of Information Act (2000) compliance
- Assisting in the formulation of any information governance / security related policies and procedures and monitoring of compliance
- Producing Trust standards, procedures and guidance on information governance / security matters for approval by the Executive Team and / or Trust Board
- Co-ordinating breaches in information governance / security, ensuring the appropriate Security Incident Forms are completed for each breach, and assessing the nature of such incidences, carrying out investigations where appropriate and considering what recommendations can be made
- All information Governance related activities.
- Agreeing and supporting organisation-wide information security initiatives, e.g. information security awareness programmes.

- Promoting and supporting the development of information security standards and procedures related to information governance.
- Attending the Information Governance Steering Sub-Committee a regular basis and through the Committee maintaining the Trust's Information Governance risk register
- The Information Governance Team is responsible for the definition, implementation and monitoring of the Information Asset Management System (IAMS) and Data Flow Mapping Information Sharing Agreements and Data Privacy Impact Assessments.
- The Information Governance administrators will be responsible for the implementation and monitoring Information Governance Toolkit Standards and for the yearly returns to the Department of Health registering the Trust's compliance to the Standards.

## 2.7 Information Security Officer

2.7.1 The Associate Director of IT Strategy & Projects is the Trust's designated Information Security Officer.

They will work closely to ensure the implementation of information governance / cyber security practices across the organisation.

2.7.2 These Trust officers will also be responsible for the dissemination of staff awareness and training programmes in relation to information governance / security.

2.7.3 Attending the Information Governance Steering Sub-Committee on a regular basis and through the Committee maintaining the Trust's Information Security risk register.

## 2.8 Data Protection Officer

2.8.1 The Data Protection Officer is responsible for:

- Ensuring that appropriate Data Protection Act notifications are maintained for applicable Trust's systems and information.
- Dealing with enquiries, from any source, in relation to the GDPR, Data Protection Act and facilitating advice and support relating to formal subject access requests.
- Advising users of information systems, applications and networks on their responsibilities under the Data Protection Act, including subject access requests.
- Advising the Director of Information Technology on breaches of the Act and the recommended actions.
- Encouraging, monitoring and checking compliance with GDPR and the Data Protection Act.
- Liaising with external organisations on data protection matters.
- Promoting awareness and providing training, guidance and advice on GDPR and the Data Protection Act as it applies with the Trust.
- Ensuring all training is recorded and registered appropriately.

- To be available to be contacted directly by data subjects – the contact details of the data protection officer will be published in the organisation's privacy notice
- To have no conflict of interest.

## 2.9 Information Asset Owners (IAO)

2.9.1 Each information asset or new development will be assigned an Information Owner. Owners are responsible for:

- Ensuring that security is designed and built-in to new systems before initial deployment.
- Ensuring that adequate security is put in place for assets that existed before this policy was enacted.
  - Ensuring that all assets and security processes associated with each individual system is identified, defined and documented.
  - Ensuring that authorisation levels and procedures are clearly defined and documented.
  - Ensuring that any delegated responsibility has been discharged correctly.

**IAA** - Provide support to the IAO's by:

- Ensuring that policies and procedures are followed
- Recognising potential or actual security incidents,
- Consulting the IAO on incident management,
- Ensuring that the information asset registers are accurate and maintained

## 2.10 Freedom of Information Act (FOIA) Responsibilities

2.10.1 The Legal Services Manager is the Trust Freedom of Information Officer and is responsible for:

- The central information access function, ensuring FOIA requirements are met.
- Providing professional advice and support on the release of information under the FOIA, researching and keeping up-to-date with legislation to ensure all advice is in line with legal requirements.
- Providing training and education awareness, undertaking presentations and workshops as appropriate to ensure all staff are aware of their responsibilities.

## 2.11 Associate Director of Systems & I.G

2.11.1 The **Associate Director of Systems & I.G** will be responsible for the implementation of the IT facility procedures detailed within this policy and its associated procedural guidelines.

2.11.2 The **Associate Director of Systems & I.G** will be responsible for ensuring information governance / security is considered when applications / systems are under development or enhancement.

## 2.12 Line Manager's Responsibilities

2.12.1 Line managers are directly responsible for:

- Ensuring the security of the Trust's assets, that is information, hardware and software used by staff and, where appropriate, by a third party, is consistent with legal and management requirements and obligations.
- Ensuring that this policy and its supporting procedures and guidelines are built into local processes and that their staff are aware of their security responsibilities and there is on-going compliance and adherence within their teams.
- Ensuring that their staff have had suitable mandatory information governance / security training.

## 2.13 General / All Staff Responsibilities

2.13.1 All staff, whether permanent, temporary, bank or contracted (including contractors), are responsible for ensuring that they are aware of the mandatory requirements placed upon them, and for ensuring that they comply with the appropriate Trust procedures in relation to information governance / security and that it becomes an integral part of the day to day operations of the Trust.

2.13.2 All staff, or agents acting for or on behalf of the Trust, have a duty to:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the Trust's IT systems.
- Report on any actual or suspected breaches in information governance / security of this policy or its associated procedures; any weaknesses or potential threats to information governance / security. These breaches should be reported either on Datix and/or directly to their immediate line manager and the Information Governance Manager / Information Governance Officers as quickly as possible. Security incidents are not limited to "hacker activity" but include any incident that has / can cause harm to information assets, for example, operator errors and service outage.
- Act in an ethical and professional manner and ensure that all activities are conducted in a security conscious manner.
- Undertake mandatory information governance / security training on an annual basis.

### ***Responsible Committees***

## 2.14 Trust Board Responsibilities

2.14.1 There is Trust Board representation on the Information Governance Steering Sub-Committee to ensure that information governance is embedded within the Trust's structure.

## 2.15 The Quality Committee Responsibilities

2.15.1 Information Governance Management across the Trust will be co-ordinated by the Information Governance Steering Sub-Committee, which is accountable to the Trust Board.

## 2.16 Information Governance Group Responsibilities

2.16.1 The Trust's Information Governance Steering Sub-Committee has the responsibility for overseeing the implementation of the Information Governance Framework, the Information Governance Policy and the Information Governance Toolkit Assessment Plan.

## 2.17 Trust Records Group Responsibilities

2.17.1 The Trust's Records Group reports to the Information Governance Steering Sub-Committee to ensure information governance in relation to records management is embedded within the Trust's structure.

## 3.0 DEFINITIONS

### 3.1 Information Governance

- A framework which allows organisations and individuals to ensure that confidential information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. It brings together all of the requirements, standards and best practice that apply to the handling of information.

### 3.2 Data Security & Protection Toolkit (DSPT)

- The web based application available via the NHS network which has been jointly developed by the Department of Health and the NHS Digital incorporating initiatives relating to matters such as confidentiality, data protection, freedom of information, information security, information quality assurance and health records management.

### 3.3 Senior Information Risk Owner (SIRO)

- An Executive member of staff that sits on the Board who will have overall responsibility for Information risk for the Trust.

### 3.4 Personal Identifiable Information

- Described in Article 4 - Definitions (GDPR) as factual information or expression of opinion which relates to an individual who can be identified from that information or in conjunction with any other information coming into possession of the data holder. Personal information includes; name, address, postcode, date of birth, staff details or any other unique identifier such as NHS Number, Hospital Number, National Insurance Number etc. It also includes information which, when presented in combination, may identify an individual e.g. Postcode, date of birth etc.

### 3.5 Sensitive Information

- Defined in Article 9 (GDPR) - special categories of personal data as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings genetic, biometric or convictions. These sets of data are subject to more stringent conditions on their processing when compared to personal identifiable information.

### 3.6 Confidential Information

- Any information if leaked into the Public domain that could harm an individual or an Organisation.

## 4.0 PRINCIPLES

- 4.1 The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information / data. The Trust fully supports the principles of Information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard both personal information about patient and staff and commercially sensitive information.
- 4.2 The Trust also recognises the need to share information with other health organisations and other agencies in a controlled manner, with the interests of the patient / staff, and in some circumstances, the public interest.
- 4.3 The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in the decision making process.
- 4.4 There are four key connecting components to the information governance / security policy and its associated procedures:
- Openness
  - Legal compliance
  - Information security
  - Information quality assurance

#### 4.4.1 Openness

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust code of openness.
- The Trust will establish and maintain policies and procedures to ensure compliance with the Freedom of Information Act.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.

- Patients will have ready access to information relation to their health care, their options for treatment and their rights as patients.
- Staff will have ready access to information in relation to their personnel records.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will have clear procedures and arrangements for handling queries from patients, staff and the public.

#### 4.4.2 Legal Compliance

- The Trust regards all identifiable personal information relation to patients and staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act and the common law on confidentiality.
- The Trust will establish and maintain policies and procedures for the controlled and appropriate sharing of patient / staff information with other agencies, taking account of relevant legislations (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

#### 4.4.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures, training and awareness.
- The Trust will establish and maintain incident reporting procedures, and will monitor and investigate all reported instances of actual potential breaches of confidentiality and security.

#### 4.4.4 Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records through its Records Management policy and procedures.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers will be expected to take ownership of, and seek to improve, the quality of information within their services.
- Data standards will be set through clear and consistent definitions of data items, in accordance with national standards.

- The Trust will promote information quality and effective records management through policies, procedures / users manuals and training.

It also aims to support the requirements of:

- **Accountability:** accounting for the actions of individuals by monitoring their activities.
- **Non-Repudiation:** legally acceptable assurance that transmitted information has been issued from and received by the correct, appropriately authorised, individuals

All parts of the organisation are responsible for making sure that information is protected adequately. Senior management recognise the sensitive nature of the information that the organisation stores and processes, and the serious potential harm that could be caused by security incidents affecting this information. They will therefore give the highest priority to information security. This will mean that security matters will be considered as a high priority in making any business decisions. This will help the Trust to allocate sufficient human, technical and financial resources to information security management, and to take appropriate action in response to all violations of Security Policy.

## **5.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE**

5.1 It is the policy of the Trust to ensure that all staffs, and partner organisations, comply with any statutory obligations relating to information governance / security.

### **5.2 Identification of Relevant Legislation**

5.2.1 The Trust will ensure that for each of its information systems it has identified all relevant statutory, regulatory and contractual requirements pertaining to the systems, and that individual responsibilities to meet these requirements are defined within the appropriate job descriptions.

5.3 Any use of personal identifiable information must comply with the legislation listed below; enquiries should be addressed to the Data Protection Officer or Information Governance Manager:

- General Data Protection Regulation
- The Data Protection Act (2018)
- The Freedom of Information Act (2000)
- The Human Rights Act (2000)
- The Common Law Duty of Confidentiality
- The Copyright, Designs and Patents Act (1990)
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Health and Social Care Act (2000) (*this list is not exhaustive*)

#### **5.4 Control of Proprietary Software Copying**

5.4.1 The Copyright Designs and Patents Act 1988 controls the copying of software. No copyright material will be copied without the copyright owner's consent. All enquiries are to be addressed to the Head of IT.

#### **5.5 Safeguarding of Trust Records**

5.5.1 The Trust will ensure that important records are protected from loss or destruction. This will include, but will not necessarily be limited to, records that must be retained to meet statutory requirements and those records required to support the Trust's essential business activities.

5.5.2 Guidance for the appropriate storage, retention and destruction of records within the Trust is provided in the Storage, Retention and Destruction of Records Procedure. Any enquires should be addressed to the Records Manager.

#### **5.6 Data Protection and Privacy of Personal Information**

5.6.1 The Trust's Data Protection Officer is also the Legal Services Manager, who will ensure that appropriate controls are in place to protect the privacy of personal information in accordance with the requirements of the General Data Protection Regulation and the Data Protection Act 2018.

5.7 All employees of the Trust must be aware of the requirements of the legislation. It is the responsibility of all senior managers (Information Asset Owners) within the Trust to ensure that any current or proposed use of personal information within their area of responsibility complies with the Trust's Data Protection registered purposes.

#### **5.8 Caldicott Recommendations**

5.8.1 The Trust will comply with the recommendations of the Caldicott Report into the use of patient identifiable information within the NHS. All uses of patient identifiable information within the Trust must comply with the Caldicott principles of good practice. Any enquiries should be addressed to the Caldicott Guardian.

#### **5.9 Information Sharing**

5.9.1 The sharing of confidential patient-identifiable information should be governed by clear and transparent procedures that satisfy the requirements of law and guidance and regulate working practices in both the disclosing and receiving organisations. In some circumstances these procedures and the underpinning standards should set out within an agreed information sharing agreement or protocol. A Data Privacy Impact Assessment is also required to assess risk to any data transfers or change of use/ implementation of a new system or change to a system. Both will identify the legal basis for sharing data appropriate to the purpose.

5.9.2 The Trust will need to share confidential patient-identifiable information with a range of organisations. The purpose to be served by sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes e.g. service evaluation, patient complaints or care enquiries, research, finance, public health work etc.

5.9.3 Information sharing agreements can be a useful way of providing a transparent and level playing field for organisations that need to exchange information. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing patients about the possibility of sharing and the choices they have to limit sharing. If the patients say no to sharing, then information may only be shared in exceptional circumstances. The lawful basis for sharing must be ascertained in all circumstances.

5.9.4 Information partners can be, but not limited to:

- NHS Organisations
- Social Care and other Local Authority elements
- The Police
- Sure Start Teams
- Education Services
- Voluntary Sector Providers
- Private Sector Providers

5.9.5 All information sharing agreements will be regularly reviewed and updated. The identification, documentation and protocols for sharing patient-identifiable information will be agreed with all new information sharing partners.

5.9.6 Please refer to the Trust's Information Sharing & Consent Policy/Procedure for additional guidance on information sharing.

## 5.10 **Prevention of Misuse of IT&T Facilities**

5.10.1 All employees of the Trust (those working for or on behalf of the Trust) and any third party users will not be granted access rights to any Trust system unless formal authorisation has been given by the IT&T Department.

5.10.2 Failure to comply with this could be in breach of the Computer Misuse Act 1990, which may lead to disciplinary action in accordance with Trust Policy.

## 5.11 Year on Year Improvement Plan and Assessment

5.11.1 An assessment of compliance with requirements, within the Information Governance Toolkit will be undertaken each year. The results of the return will be monitored along with any action / development plan by the Information Governance Steering Sub-Committee. The Executive Chief Finance Officer (SIRO) will report on the progress of the Trust against the Toolkit to the Quality Committee. The annual assessment will be submitted to the Quality Committee for ratification. The requirements are grouped into the following initiatives;

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information assurance

5.11.2 Trusts are required to complete annual self-assessments against the Information Governance Toolkit requirements by 31<sup>st</sup> March each year.

## 6.0 SCOPE OF POLICY

- 6.1 This document applies Trustwide to all services and employees of EPUT without exception.
- 6.2 This policy and its associated procedural guidelines applies to and must be read and observed by all staff, including contracted, non-contracted, temporary, honorary, secondments, bank, agency, students, volunteers or locums, wishing to use the Trust's information / data facilities and / or systems, prior to their doing so.
- 6.3 This policy and its associated procedures cover all information / data systems purchased, developed and managed by, or on behalf of EPUT and all individuals directly employed or otherwise by the trust.
- 6.4 For the purpose of this policy and its associated procedures information / data is defined as information / data that is stored in any media, for example:
- Paper
  - Electronic
  - Audio or visual
  - Passed on verbally
- 6.5 This policy and its associated procedures cover all aspects of information / data, including:
- Patient / client / service user
  - Personnel / staff
  - Organisational / corporate

6.6 This policy and its associated procedures cover all aspects of information / data, including:

- Structured record systems (paper and electronic)
- Unstructured information (paper and electronic)
- Transmission of information (fax, e-mail, post, telephone, internet)

6.7 It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

## **7.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT**

7.1 The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust.

7.2 The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate.

7.3 The Executive Chief Finance Officer (SIRO) & Clinical Support is the specific senior manager responsible for co-ordinating, publicising and monitoring implementation of this policy and its associated procedural guidelines.

7.4 This policy and its associated procedural guidelines will be reviewed every three years in line with Trust policy or whenever legislation, national or local guidance requires.

7.5 The Information Governance Manager, Information Security Officers and Information Asset Owners (as defined within the Trust's Information Asset Register held by the Information Governance Leads) will be responsible for ensuring the implementation of this policy and its associated procedures, as appropriate.

7.6 The Information Governance Manager and / or Information Security Officer will provide the Information Governance Steering Sub Committee, Quality Committee and Executive Team with relevant reports on information governance / security developments, breaches, changes in legislation / guidance and facility usage on a regular basis (minimum quarterly).

7.7 The Trust will work towards full and continued compliance to information security management systems, ensuring independent audits are undertaken, as appropriate or dictated by guidance:

- Information Governance Toolkit (IG Toolkit) standards
- Care Quality Commission (CQC)
- Internal Auditors
- NHS Litigation Authority (NHSLA)

**8.0 ABUSE OF TRUST FACILITIES**

- 8.1 Any employee found to be in breach of information governance / security guidance may be investigated pending disciplinary procedures in line with Trust policy and may be subject to formal proceedings.
- 8.2 In the event of abuse of any Trust information / data systems / services all access will be immediately revoked pending any investigation. This will include:
- the deliberate accessing, viewing, downloading or distributing of:
    - Information not related to role (e.g. accessing their own / friends / family information).
    - Pornographic or otherwise offensive material.
  - the use of portable media (i.e. laptops, USB Keys, mobile phones, PDA etc.) to store / transfer person identifiable data.
  - not adhering to clear desk policy (safe, secure storage of manual records in empty offices).
- 8.3 Such acts would be regarded as gross misconduct under the Trust's disciplinary procedures and the use / transfer of person identifiable or sensitive data / information outside of Trust procedures. Any employee found to have been engaging in such activities will be investigated through the disciplinary procedures in line with Trust policy and may be subject to formal proceedings.

**9.0 TRAINING**

- 9.1 The Trust will maintain a high level of information governance / security awareness within the organisation by ensuring that all staff receive appropriate, job relevant, training. This may include:
- Team Briefings
  - Publications via Electronic Staff Briefings
  - On-Line training via the NHS DIGITAL Information Governance website.
  - OLM Training
  - It will be a mandatory requirement for all staff involved in any type of information governance / security breach to complete training, irrespective of previous sessions.
  - Training will be done in accordance with the Induction and Mandatory Training Policy.

**10.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES**

Information Governance/Security Procedural Guidelines

CPG50 – Information Governance & Security Procedure  
CPG50A – ITT Security Procedure  
CPG50B – Email, Intranet, Internet Access & Use Procedure  
CPG50C – Safe Haven Procedure  
CPG50D – Information Governance Incident Reporting Procedure  
CPG50E – Data Privacy Impact Assessment Procedure  
CPG50F – SMS Text Messaging to Service Users Procedure  
CPG50G – Information Asset Register Procedure  
CPG50H – NHSMail Usage Procedure  
CPG50I – Not used

**END**

SAMPLE ONLY

## USE OF MOBILE PHONES POLICY

<b>POLICY REFERENCE NUMBER:</b>	CP54
<b>VERSION NUMBER:</b>	2
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	Full 3 year review
<b>AUTHOR:</b>	██████████ Advancing Clinical Practice Lead
<b>CONSULTATION GROUPS:</b>	Trust wide: Operational Managers Estates & Facilities Compliance & Risk Team Mobius / Paris Team Pharmacy
<b>IMPLEMENTATION DATE:</b>	01 April 2017
<b>AMENDMENT DATE(S):</b>	May 2018; February 2020
<b>LAST REVIEW DATE:</b>	April 2020
<b>NEXT REVIEW DATE:</b>	April 2023
<b>APPROVAL BY CLINICAL GOVERNANCE &amp; QUALITY SUB-COMMITTEE:</b>	February 2020
<b>RATIFICATION BY QUALITY COMMITTEE:</b>	April 2020
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be produced in whole or in part with the permission of the copyright owner.

<b>POLICY SUMMARY:</b>		
<p>The purpose of this policy and accompanying procedural guidelines is to set out working arrangements for the use of Mobile Phones within all areas of Trust premises for Staff, Patients and Visitors.</p> <p>The use of Mobile Phones within patient settings must include a local individual risk assessment which considers whether use would represent a threat to patients', staff and/or visitors safety or that of others. Risk Assessments must include the consideration of the operation of individual phones together with any surrounding electrically sensitive medical devices in critical care situations and privacy and dignity. 'Patient' will be the terminology used throughout this document and will refer to a patient, resident or service user.</p>		
<b>The Trust monitors the implementation of and compliance with this policy in the following ways;</b>		
<p>This policy and procedural guideline will be reviewed and monitored for compliance initially for a minimum of 1 year and thereafter 3 yearly or as required by legislation/best practice guidelines.</p> <p>Following an incident where a mobile phone interferes with medical equipment this must be reported on an Incident Reporting Form and returned to the Integrated Risk Team. The Integrated Risk Team will then be responsible for reporting this to the MHRA and NPSA as required.</p>		
<b>Services</b>	<b>Applicable</b>	<b>Comments</b>
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is  
Executive Director of Nursing**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

USE OF MOBILE PHONES POLICY

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

- 1.0 INTRODUCTION
- 2.0 SCOPE
- 3.0 RESPONSIBILITIES
- 4.0 LEGAL CONSIDERATIONS
- 5.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE
- 6.0 REFERENCES
- 7.0 REFERENCE TO OTHER TRUST POLICIES

SAMPLE - DO NOT USE

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

USE OF MOBILE PHONES POLICY

1.0 INTRODUCTION

- 1.1 Communication with family and friends is an essential element of support and comfort for patients either in hospital or whilst receiving care as an outpatient. Modern technology has made communication relatively easy particularly with the widespread use of mobile phones, text messaging and email. The use of mobile phones by staff, patients and visitors presents an increasing challenge due to new and continually developing technologies, potential connection and interaction to other hardware devices and portability. (DOH January 2009)
- 1.2 Mobile Phones commonly have extended functionality which can include email, internet, camera, audio or video recording capability and music players. Therefore, there is a potential for patients and visitors to use these functions to take inappropriate photographs, recordings or videos. This has a potential to present the greatest interference with patient dignity and privacy.
- 1.3 NHS Protect, which was replaced by NHS Counter Fraud Authority in 2017, produced good practice advice in the May 2016 Patients Recording NHS staff in Health and Social Care Settings document which covers both covert and overt recording of consultations. Clarification of this document is cited in the Trust Mobile Phone Procedure CPG54.
- 1.4 Ring tones or music played via mobile phones could disturb others who are trying to recuperate and constant 'chatter' of staff, other patients or visitors on mobile phones would be equally disruptive.
- 1.5 Mobile phones could equally interfere with medical equipment and affect their use.
- 1.6 In addition charging mobile phones requires the use of a length of electrical wire which may provide ligature risks.
- 1.7 Consideration of these issues is essential in regards to where mobile phones should and should not be used on Trust premises.

2.0 SCOPE

- 2.1 This Policy and associated procedural guidelines applies to all staff, patients and visitors in all Trust areas, including in community residential areas, day hospitals, resource centers and inpatient settings.
- 2.2. The possession or use of mobile phones is strictly prohibited to all staff, patients, contractors and visitors **entering clinical areas** at Edward House, Christopher Unit, Larkwood Ward, Hadleigh Unit, Brockfield House, Robin Pinto Unit, Woodlea Clinic. When entering patient areas in these units, mobile phones should either be left in staff vehicle, at home or placed in the lockers within the reception area. However, where someone needs use of a mobile phone for work related tasks then permission must be requested via security

## CP54 USE OF MOBILE PHONES POLICY

or in their absence one of the integrated clinical leads/unit coordinator for their authority. Those not working in any clinical areas of the secure wards at Edward House, Christopher Unit, Larkwood Ward, Hadleigh Unit, Brockfield, Robin Pinto and Wood Lea are able to take their mobile phone into non patient areas only. Staff in Larkwood Ward and on Poplar Ward in Rochford must read this policy in conjunction with the Unit's protocols on the use of Mobile phones.

- 2.3 The use of camera phones within patient areas or patient's own home risks infringing patient confidentiality. Given the difficulty in detecting usage, the consent for taking photographs on a mobile phone of either patients or their confidential information is prohibited. The only exception to this is for staff where a job role or function demands this use, for example in community health services staff take wound photographs for monitoring healing and the Risk Team when conducting inspections and incident follow up work.

### 3.0 RESPONSIBILITIES

- 3.1 All staff are responsible for adhering to this policy and associated procedural guidelines and for reporting any breaches on Datix reporting incident system. (please see Corporate Policy CP3 for further details)
- 3.2 All Managers have a responsibility to ensure that standards are maintained as set out in this policy and accompanying procedural guidelines.
- 3.3 All Managers are responsible for ensuring that information about this policy and procedure is available in their areas to staff, patients and visitors.
- 3.4 The responsibility for using a mobile device remains with the authorised user.
- 3.5 All operational support issues must be reported to the ITT Service Desk for resolution.
- 3.6 All mobile ITT equipment must be approved by ITT Services and will only be issued for the sole use of the recipient individual.
- 3.7 Mobile devices must be returned to ITT Services when their intended use by the recipient individual no longer applies. Devices must not be passed on to other members of staff.

### 4.0 LEGAL CONSIDERATIONS

#### 4.1 Patient Privacy and Dignity

There is a legal duty to respect a patient's private life. The Human Rights Act 1998 (HRA) enshrines the right to respect for private and family life and states "there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."

The European Commission has found that the collection of medical data and maintenance of medical records fall within the sphere protected by the HRA. This would, therefore, apply to personal medical information including information which identified a patient such as a photograph.

Permitting the use of mobile phones with cameras in hospitals may not sufficiently ensure medical confidentiality or protect an individual's right to respect for their private life.

Cameras and voice recording facilities should not be used in any way that could cause harm or offence to an individual (member of staff or client) or bring the Trust into disrepute. Under no circumstances should photos or voice recordings be taken without the prior consent of those involved. Such misuse may be subject to the Trust's disciplinary procedures and could also be subject to civil and criminal proceedings.

The risk of breaching confidentiality and dignity must be assessed against patients' rights to communicate with the outside world whilst in hospital, including access to alternative forms of communication where the use of mobile phones is not allowed.

### **4.2 Patient Confidentiality**

The Information Commissioner's Office states that all public and private organisations are legally obliged to protect any personal information that they hold. In relation to this, any individual who takes a photograph of another individual will be processing personal data and must comply with the General Data Protection Regulation 2016 (GDPR).

The use of mobile phones can result in the creation of sensitive personal data and therefore consideration must be given to how effective confidentiality is by monitoring.

### **4.3 Child Protection**

The Children Act 2004 places a duty on the Trust for ensuring the need to safeguard and promote the welfare of children. As such it must be taken into account that mobile phones are a potential risk in that inappropriate photographs/information could be taken, including confidential information pertaining to the child.

### **4.4 Health and Safety**

Mobile phones need to be charged via the mains power supply. Only approved chargers compatible with the make and model of the phone may be used when charging mobile phones on Trust premises. Whether Trust or personal property, the charger must be up to date in relation to Portable appliance testing (PAT) before permitted for use. Failure to observe this requirement will contravene Health and Safety Regulations and could place individuals at risk.

## 5.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

- 5.1 This policy and procedural guideline will be reviewed and monitored for compliance every 3 years or as required by legislation/best practice guidelines.
- 5.2 Following an incident where a mobile phone interferes with medical equipment this must be reported via the Datix Incident Reporting system. The Integrated Risk Team will then be responsible for reporting this to the MHRA and NPSA as required.

## 6.0 REFERENCES

- 6.1 The Medicines and Healthcare products Regulatory Agency (MHRA) advises that in certain circumstances the electromagnetic interference from mobile phones can interfere with some devices, particularly if used within 2 meters of such devices. It has issued a number of reference documents relating to this;
- DB 1999(02) Emergency service radios and mobile data terminals: compatibility problems with medical devices. This document covers the impact of radio communications on the safe use of medical devices.
  - DB 9702 Electromagnetic Compatibility of Medical Devices with Mobile Communications. This device bulletin includes the findings of a study conducted into the effects of mobile communications.
  - Safety Notice 2001(06) - Update on Electromagnetic Compatibility of Medical Devices with Mobile Communications: TETRA (Terrestrial Trunked Radio Systems) and Outside media broadcasts from hospital premises.
- 6.2 Using Mobile Phones in NHS Hospitals (DOH January 2009).
- 6.3 The Human Rights Act 1998 (HRA) enshrines the right to respect for private and family life set out in the European Convention on Human Rights (Convention).

### Further references:

- NHS Protect, Patients recording NHS staff in health and social care settings (March 2016)
- [http://www.cqc.org.uk/sites/default/files/20150212\\_public\\_surveillance\\_leaflet\\_final.pdf](http://www.cqc.org.uk/sites/default/files/20150212_public_surveillance_leaflet_final.pdf).
- Department of Health, 'Using mobile phones in NHS hospitals', (2009).
- [http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod\\_consum\\_dh/groups/dh\\_digitalassets/@dh/@en/documents/digitalasset/dh\\_092812.pdf](http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_092812.pdf).
- NHS Protect – Misuse of Social Media to Harass, Intimidate or Threaten NHS Staff May 2016.

**7.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES**

- Adverse Incident Serious Incidents Policy CP3 and CPG3
- Security Policy and Procedural Guidelines RM09 and RMPG09
- Purchase and Use of Mobile Phones and Pagers CP7 and CPG7
- Records Management Policy and Procedures CP9
- IT & T (Information Technology and Telecommunications) Security Policy and Procedural Guidelines CP50
- Patient/Client Property and Money Procedure FP09/02

**END**

SAMPLE - DO NOT USE

# INFORMATION GOVERNANCE & SECURITY PROCEDURE

<b>PROCEDURE NUMBER:</b>	CPG50
<b>VERSION NUMBER:</b>	3
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	3 year review; Minor amendments
<b>AUTHOR:</b>	Information Governance Team
<b>CONSULTATION GROUPS:</b>	IGSSC
<b>IMPLEMENTATION DATE</b>	April 2017
<b>AMENDMENT DATE(S)</b>	July 2018; September 2021
<b>LAST REVIEW DATE</b>	September 2021
<b>NEXT REVIEW DATE</b>	September 2024
<b>APPROVAL BY IGSSC</b>	August 2021
<b>RATIFIED BY QUALITY COMMITTEE</b>	September 2021
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2017-2021. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

PROCEDURE SUMMARY		
<p>The purpose of these procedural guidelines is to establish the governance arrangements and responsibilities for information security providing a framework through which the elements of information governance / security will be met. This will make sure that the intention to promote and build a level of consistency across the Trust to safeguard information is achieved and ensure it is understood and that all Trust staff are aware of their individual responsibilities.</p> <p>The risk associated with not having a procedure document in relation to information governance / security and access to Trust facilities (IT, Email, Internet, Portable Media) is an uncoordinated approach to its safe use which could render the Trust vulnerable in terms of legal implications of staff use of facilities and lack of organisational controls to safeguard users and the Trust.</p>		
<b>The Trust monitors the implementation of and compliance with this procedure in the following ways;</b>		
<p>The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate.</p>		
<b>Services</b>	<b>Applicable</b>	<b>Comments</b>
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is  
The Executive Chief Finance Officer**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**INFORMATION GOVERNANCE & SECURITY PROCEDURE**

**CONTENTS**

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

**1.0 INTRODUCTION**

**2.0 GENERAL INFORMATION**

**3.0 IMPLEMENTATION AND MANAGEMENT**

**4.0 RISK**

**5.0 TRAINING**

**6.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT**

**7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION**

SAMPLE ONLY

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**INFORMATION GOVERNANCE & SECURITY PROCEDURE**

**Assurance Statement**

**1.0 INTRODUCTION**

- 1.1 These procedural guidelines aim to set out the Essex Partnership University NHS Foundation Trust's (the "Trust") rules relating to information governance / security and apply to all business functions and cover all information systems, networks, physical environment, third party contractors, and relevant people who support those business functions.
- 1.2 The information used by the Trust is an important business asset in terms of both the clinical management of individuals and the efficient management of services and resources and the substantial personal and confidential information relating to patients, the public and employees that the Trust is required to hold and manage. It is vital that the confidentiality, integrity and availability of information / data is maintained. Information governance / security deals with the way an NHS Trust handles personal and sensitive information / data and allows the organisation and individuals to ensure that such information is dealt with in line with legislation, securely, efficiently and effectively and in doing so preserving the Trust's reputation.
- 1.3 Increasing reliance is placed on technology, computers and, to an extent, third party contractors, to store and manage information, and with innovative ways by which information can be communicated, it is at a greater risk. It is therefore important that the Trust follows a consistent approach to safeguard its information, with due regard to the sensitive nature of some held, both in electronic and manual systems.
- 1.4 The principle objective of information governance / security management is to implement appropriate administrative, technical and physical safeguards to ensure the security of these assets.

**2.0 GENERAL INFORMATION**

- 2.1 It is the policy of the Trust that all information / data systems operated by the Trust (electronic or manual) are secure systems, which comply with the requirements of the UK General Data Protection Act, Data Protection Act 2018, the Computer Misuse Act, the British Standard for Information Security ISO/IEC 27000 series (using the International Standard Organisations Code of Practice ISO27002) and the Data Security & Protection Toolkit, as appropriate. It is the aim of the Trust that its entire staff will be aware of the need to maintain secure systems and that staff will fully understand their responsibilities as outlined in these procedural guidelines.

- 2.2 Line managers will be responsible for ensuring that their staff are aware of these procedures and their contents and for ensuring that their staff abide by them. Line managers will ensure staff are compliant with the Trust OLM Information Governance training.
- 2.3 Failure by any employee of the Trust to abide by the contents of this document will be viewed as a serious matter and may result in disciplinary action.
- 2.4 This document sets out the Trust processes for the safe and legal use of the facilities provided by the Trust, for example, internet / Email access, IT and portable media and paper / manual processes and should be read and observed by any member of staff using these facilities.

### **3.0 IMPLEMENTATION & MANAGEMENT**

- 3.1 Information governance / security is not just a matter of restricting unauthorised access to information / data, it is also a question of ensuring that the confidentiality, integrity and availability of the information / data is maintained.
- 3.2 The appendices attached to these procedural guidelines will provide detailed information on the processes to be followed to ensure that information governance / security guidance is met in relation to:
- Integrated Governance Strategy
  - Information Governance Framework
  - Records Strategy
  - IM&T Security Policy
  - Virtual Private Network (VPN) Remote Access Policy / Procedures
  - Data Protection and Confidentiality Policy / Procedures
  - Freedom of Information Policy / Procedures
  - Health Records Management Policy / Procedures
  - Data Quality Policy
  - Closed Circuit Television (CCTV) Policy / Procedures
  - Information Governance and Security Policy
  - IT&T Security Procedures
  - Internet/Intranet/Email Access and Use Procedures
  - Incident Reporting Procedures
  - Information Sharing and Consent Policy / Procedures
  - Paper and Electronic Corporate Records (Laserfiche) Policy / Procedures

*This list is not exhaustive....*

## 4.0 RISK

- 4.1 The Director of ITT will ensure that each of the Trust's systems is subject to regular security risk assessments. The degree of detail of the assessment will depend on the value of the asset(s). All reports produced will remain confidential.
- 4.2 To ensure compliance of systems with NHS security policies and standards the Trust will ensure that the security of IT&T systems will be regularly assessed. Risk assessments will be regularly carried out and the technical and IT&T facilities checked for compliance with ISO/IEC 27000 series - Information Security Management, the Code of Practice for information Security, which forms the basis of the NHS security policy.
- 4.3 Key leads will manage risk by identifying, controlling and minimising risk to an acceptable level, by undertaking appropriate risk assessment processes to assess threats, vulnerabilities and the resulting impact upon information assets.
- 4.4 Any risk that cannot be reduced to an acceptable level by imposing existing Trust controls (e.g. policy, procedure, process) will be escalated to the Information Governance Steering Sub-Committee / Quality Committee as appropriate and entered onto the information governance / security risk register for monitoring by same.
- 4.5 The processes involved in risk analysis will be to identify and value the asset(s), threats and vulnerabilities and then calculate the risk.

### 4.6 Countermeasures

- 4.6.1 Introducing 'countermeasures' will involve identifying, selecting and adopting appropriate and cost-justified security and contingencies in order to reduce risks to an acceptable level.
- 4.6.2 These 'countermeasures' may act in different ways, including:
- Reducing the likelihood of attacks or incidents occurring.
  - Reducing the system's vulnerability.
  - Reducing the impact of an attack or incident, should it occur.
  - Detecting the occurrence of attacks or incidents.
  - Assisting the progress of recovery from an attack or incident.
- 4.6.3 The Security Officer will regularly re-examine the use of any countermeasures and their continuing suitability and effectiveness. A report will be produced following any assessment.

## **5.0 TRAINING**

- 5.1 All Trust staff will undertake, as part of their general induction, mandatory training on information governance, cyber security and related areas such as confidentiality, Data Protection, record keeping.
- 5.2 Specific staff training will be undertaken by those staff appointed with key roles in relation to information governance / security, e.g. Information Governance Managers / Information Security Officers and Information Asset Owners.
- 5.3 All mandatory training will be recorded for monitoring purposes. Reference should be made to HR21 – Induction and Mandatory Training Policy and related Procedures.

## **6.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT**

- 6.1 The Quality Committee will have overall responsibility for overseeing the implementation of these procedural guidelines and will take forward any action relating to information governance / security within the Trust.
- 6.2 The Information Service Management Board and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of these guidelines.
- 6.3 These procedural guidelines will be reviewed every three years in line with Trust policy unless changing circumstances or central policy requires an earlier review.
- 6.4 The Information Governance Manager and / or Information Security Officers will provide the Quality Committee, the Executive Team and Board of Directors with relevant reports on information governance / security developments, breaches and facility usage on a regular basis, in line with Committee schedules.
- 6.5 Trust information governance leads will undertake internal audit of staff awareness of information governance / security on a yearly basis via the media of staff questionnaires. Outcomes of these audits will be reported to the Information Governance Steering Sub-Committee for action planning to address any gaps.
- 6.6 The use and any misuse / abuse of the Trust's electronic facilities (e.g. Email, Internet) will be monitored by the IT&T department and outcomes will be provided to the Executive Team as part of the Performance Department's Quarterly Performance Monitoring Report.
- 6.7 Any breaches in information governance / security will be investigated in line with Trust policy (Serious Untoward Incidents [CP3/CPG3], Information Incident Reporting Procedures (CPG50) and / or Disciplinary Policy [HR27/HRPG27]) and reported through the Information Governance Steering Sub-Committee / Caldicott Network as appropriate. The Caldicott Network will be responsible for:

- escalating any issues to the Quality Committee
- ensuring the actioning and publication of lessons learned following any breach investigations across the Trust

## **7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION**

7.1 This document should be read in conjunction with other national guidance, Trust policies and procedures and other relevant legislation, including:

- Information Quality Assurance
- British Standard for Information Security ISO/IEC27000 series
- NHS Caldicott Report Recommendations
- The National Health Service Act (2006)
- Data Protection Act (2018)
- Access to Health Records Act (1990) (Where not superseded by the Data Protection Act (2018))
- Freedom of Information Act (2000) (FOI) (including Publication Scheme)
- The Environmental Information Regulations (2004) (EIR)
- Computer Misuse Act (1990)
- Electronic Communications Act (2000)
- The Re-Use of Public Sector Information Regulations (2005)
- The Civil Contingencies Act (2004)
- The Human Rights Act (2000)
- The Copyright, Designs and Patents Act (1988) (as amended by the Copyright Computer Programs Regulations (1992))
- The Health and Safety at Work Act (1974)
- Regulation of Investigatory Powers Act (2000)
- Crime and Disorder Act (1998)
- Health and Social Care Act (2000)
- The Common Law Duty of Confidentiality
- General Data Protection Regulation

***This list is not exhaustive.....***

**END**

## EMAIL/INTERNET/INTRANET ACCESS AND USE PROCEDURE

<b>PROCEDURE REFERENCE NUMBER:</b>	CPG50b
<b>VERSION NUMBER:</b>	1.8 (1 month extension QC Feb 22)
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	Minor amendment in 9.9 (new bullet)
<b>AUTHOR:</b>	
<b>CONSULTATION GROUPS:</b>	IGSSC
<b>IMPLEMENTATION DATE:</b>	May 2018
<b>AMENDMENT DATE(S):</b>	February 2019, March 19 (secure email changes); Dec 2019 (review date change); Sept 2020 (minor amendment 9.9)
<b>LAST REVIEW DATE:</b>	N/A
<b>NEXT REVIEW DATE:</b>	<del>May August November 2021</del> February March 2022
<b>APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:</b>	March 2018
<b>RATIFICATION BY QUALITY COMMITTEE:</b>	May 2018
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

<b>PROCEDURE SUMMARY</b>
These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of email and internet/intranet use is minimised and that there is a co-ordinated approach to the safe use.
<b>The Trust monitors the implementation of and compliance with this procedure in the following ways:</b>
The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate

Services	Applicable	Comments
Trustwide	✓	

**The Director responsible for monitoring and reviewing this procedure is  
Executive Chief Finance Officer**

## EMAIL/INTERNET/INTRANET ACCESS AND USE PROCEDURE

### CONTENTS

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

- 1.0 INTRODUCTION
- 2.0 AIMS & OBJECTIVES
- 3.0 RESPONSIBILITIES
- 4.0 DEFINITIONS
- 5.0 USING E-MAIL SYSTEMS
- 6.0 HOUSE KEEPING FOR E-MAIL SYSTEMS
- 7.0 SECURITY OF E-MAIL
- 8.0 CONTINUITY OF E-MAIL ACCOUNTS
- 9.0 USING INTERNET/INTRANET SYSTEMS
- 10.0 OBTAINING INTERNET/E-MAIL ACCESS
- 11.0 MONITORING INTERNET/INTRANET/E-MAIL SYSTEMS

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**EMAIL/INTERNET/INTRANET ACCESS AND  
USE**

**Assurance Statement**

These procedural guidelines will ensure that the risk associated with not having a procedural document in relation to information governance / security in regard of email and internet/intranet use is minimised and that there is a co-ordinated approach to the safe use.

**1.0 INTRODUCTION**

- 1.1 Essex Partnership University NHS Foundation Trust (the Trust) makes extensive use of electronic mail (e-mail) and internet/intranet both within the Trust and with external organisations.
- 1.2 This document is intended to define in a clear and straight-forward manner the risks and the conditions under which the Trust's e-mail and internet/intranet systems might be used.

**2.0 AIMS AND OBJECTIVES**

- 2.1 The purpose of this document is to define the procedure for use of the Trust's e-mail and internet/intranet systems. The policy applies to the Trust's employees and others carrying out work on behalf of the Trust.
- 2.2 This procedure applies equally to basic e-mail messages and to any attachments sent with messages. For ease of reading, the term e-mail is used to refer to both basic messages and to any attachments and other associated files throughout the remainder of this document.
- 2.3 The purpose of this procedure is to clearly explain what is acceptable and unacceptable when using the Internet/Intranet.

**3.0 RESPONSIBILITIES**

**3.1 *Directors must:-***

- ensure that this procedure is distributed throughout the Trust.

**3.2 *Managers must:-***

- ensure that all of their staff are aware of this procedure and understand their responsibilities under it.
- identify, and provide secure access to equipment that their staff may use to access e-mail and internet/intranet systems.
- ensure that their staff follow this procedure
- Ensure that NHS.mail accounts are cleared of Trust emails on staff leaving EPUT.

3.3 **Employees must:-**

- make themselves aware of this procedure and follow it whenever they access the internet/intranet.
- only use e-mail systems in accordance with this procedure.
- only access e-mail systems if they have been authorised to do so.
- not share the access privileges that they have been granted with others.
- not use others' access privileges to access e-mail or internet/intranet systems.
- ensure all personal e-mails are deleted from their account when leaving the Trust.
- Staff must not use their personal email for work purposes.
- NHS.mail accounts must be cleared of Trust emails on staff leaving EPUT.

3.4 **Assistant Director of I.T. Service Delivery must:-**

- ensure the continued management of information technology security.

3.5 **IT Support Staff must:-**

- only install and give access to the e-mail or internet/intranet systems after the request for access has been authorised.
- record activity by the Trust employees on e-mail or internet/intranet systems.
- regularly review the security effectiveness of the means of access.

<b>4.0 DEFINITIONS</b>
------------------------

4.1 **NHSmail**

- NHSmail should be used to send sensitive/patient/ resident identifiable information by secure (encrypted) e-mail. All staff should have an NHS.mail account.

4.2 **Patient or Residents /Personal Information**

- **“Personal Data”**

Means any information relation to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

4.3 **Sensitive Personal/Business Information**

- **“Special categories of personal data”(sensitive) Article 9**

Means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

#### 4.4 Chat Rooms

- These are social networking sites such Facebook, Myspace etc.  
(Please refer to the Social Media Policy / Procedure for further guidance)

#### 4.5 I.P. Address

- This is the unique address for your computer.

### 5.0 USING E-MAIL SYSTEMS

Only approved Trust enabled email systems can be used or NHS Mail (nhs.net).

#### **Acceptable Use:-**

- 5.1 Any e-mail address provided by the Trust, assigned by the Trust to individuals, sub-units, or functions of the Trust, is the property of Essex Partnership University NHS Foundation Trust ('The Trust').
- 5.2 Those that use Trust email services are expected to do so responsibly, that is, to comply with national laws, with this and other policies and procedures of the Trust, and with normal standards of professional and personal courtesy and conduct.
- 5.3 Access to Trust e-mail services, when provided, is a privilege that may be wholly or partly restricted by the Trust without prior notice when there is Substantiated Reason to believe that violations of law or policy have taken place, or, in exceptional cases, when required to meet time-dependant, critical operational need.
- 5.4 As e-mail messages may have to be disclosed in litigation / Freedom of Information requests, it is always good practice for users to ask themselves before sending an e-mail message how they would feel if it was read out in court / released for publication.
- 5.5 An e-mail message is, for legal purposes, treated as a publication and is therefore subject to all normal legal restrictions on publication.
- 5.6 E-mail may appear to be informal but can be used to create binding contracts and users must take due care not to enter into contractual obligations without the usual care and attention to detail necessary to protect the Trust's interests.
- 5.7 Access to e-mail will be inspected and/or monitored by Trust systems to protect the Trust, Trust Computing Facilities and account holders from e-mail borne viruses/macros/inappropriate attachments and/or content where possible.

- 5.8 All email records destined for the internet will have an email disclaimer appended to the end of the email by the Trust systems. An example below:

*"It is intended solely for the addressee. Please notify the sender immediately if you are not the intended recipient. Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.*

*Any views expressed in this email are those of the individual, and may not represent the views of Essex Partnership University NHS Foundation Trust.*

*The presence of this disclaimer indicates that the email has been virus scanned. Although this email and any attachments are believed to be free of any virus, or any other defect which might affect any computer or IT system on which they are received and opened, it is the responsibility of the recipient to ensure that they are virus free. Essex Partnership University NHS Foundation Trust accepts no responsibility for any loss or damage arising in any way from receipt or use thereof. If you received this in error, please contact the sender and delete the material from any computer."*

- 5.9 When sending Patient/ Resident/ Personal/Sensitive Identifiable Information via e-mail all documents must be password protected or sent through NHSmail. Passwords should be forwarded to recipients by telephone or text wherever possible – in emails a suitable gap should be left between the original email and the password to enhance security.
- 5.10 No Patient/Resident/ Personal/Sensitive Identifiable Information should be listed in the Subject Heading Bar. The subject window of confidential information transferring by email must be identified as "SAFE HAVEN". Best practice requires that no identifiable information is used within the body of the email unless it is absolutely essential in which case initials can be used unless these initials can identify an individual.
- 5.11 Emails must be checked to ensure that responses / replies are only sent to the relevant recipients and that the content of the email does not include irrelevant email "runs" (additional information included within the email).
- 5.12 The use of e-mail messages to send patient/resident identifiable data internally within the Trust may be undertaken only to those individuals who are authorised to receive it, when Caldicott principles have been applied and must be encrypted or password protected where possible.
- 5.13 There are many departments within the Trust that use e-mail as equivalent to an authorised and signed document. Users must be certain of the validity of the content of the mail and its sender before action is taken upon them.

- 5.14 It is understood that staff sometimes need to deal with personal / private matters during the working day. Limited personal use is therefore allowed provided it is kept to a reasonable level and does not interfere with the working day. This arrangement will be based on trust and all staff will be expected to use this facility in an appropriate manner. Staff should be aware that personal use of e-mail will be monitored.
- 5.15 The printing of e-mail messages is generally unnecessary. Users should consider developing the habit of dealing with all correspondence electronically, including on-line filing of any messages they wish to retain.
- 5.16 Data within an e-mail is predominantly confidential Trust data. As such it may be subject to the provision of Data Protection and Freedom of Information legislation.
- 5.17 E-mail distribution lists must only contain addressees who appropriate recipients of the e-mail content. E-mail **must not** be sent out to a large number of people unless essential as you could be wasting people's time and causing possible disruption to services. Do not ask for acknowledgements from distribution lists.
- 5.18 If a message is not delivered, you will receive a non-delivery report. This will normally identify the cause of non-delivery such as incorrect address, unavailable end system, etc. Look at this information first before raising a request for support as you may just need to correct the address.
- 5.19 Delivery reports indicate that the e-mail has been successfully sent and will only be returned if the sender has requested it.
- 5.20 Receipt notifications indicate that the recipient has opened the e-mail. Remember that the recipient may not have read or acted upon the e-mail, as a personal assistant or administrator may have read the e-mail on behalf of the recipient.
- 5.21 Delivery reports or read receipt notifications may incur a charge from NHSmail or other service providers, so only request these when you need positive confirmation that a message has been received and read. These types of notifications may not be available from other recipients.
- 5.22 The following email domains are secure and encrypted;
- nhs.net
  - secure.nhs.uk
  - gov.uk (no longer needs to be gsi.gov.uk)
  - cjsm.net
  - pnn.police.uk
  - mod.uk
  - parliament.uk

**Unacceptable Use:-**

- 5.23 The Trust shall permit the inspection, monitoring, or disclosure of e-mail without the consent of the account holder if e-mails contain obscene, indecent, racist or illegal content:
- when required by and consistent with law
  - when there is Substantiated Reason to believe that violations of law or of Trust Policies have taken place
  - when there are Compelling Circumstances
  - Under time-dependent, critical operational circumstances as defined in the procedural guidelines (3.0).
- 5.24 E-mail messages or attachments **not password protected** must not contain any Patient/Resident /Personal/Sensitive Identifiable Information. Sending PID by NHSMail to NHSMail is the most secure method.
- 5.25 Access to e-mail is provided for staff to use in the course of their work. Staff are prohibited to access, view, download, display or distribute any of the following:
- anything which constitutes pornography
  - anything which is sexually explicit
  - anything which is libellous
  - anything which is sexist, homophobic, racist
  - anything which is otherwise offensive.
- 5.26 Where staff inadvertently access e-mail which may fall into the group above (5.23) this should be reported to the Trust's ITT Helpdesk immediately.
- 5.27 Trust e-mail services may not be used for:
- unlawful activities
  - commercial purposes not under the auspices of the Trust
  - personal financial gain
  - relaying person identifiable information / data to home email systems for the purposes of working from home unless connected to the Trust networks via the Virtual Private Network (VPN)
  - personal use that:
    - directly or indirectly interferes with the Trust operation of computing facilities, internet or email services
    - burdens the Trust with noticeable incremental cost
    - interferes with the user's employment or other obligations to the Trust
    - gives the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the Trust, unless appropriately authorised to do so
    - employs false identity
    - creates, sends, forwards or replies to inappropriate material including, but not limited to, graphics, video clips, jokes, viruses and music files

- inappropriate use of email distribution lists (emails should be targeted to specific groups rather than to All Trust Staff. Trust Intranet Bulletin Boards should be used for general information relating to, e.g. surplus equipment)
- or uses that violate other Trust policies or guidelines
- the latter include, but are not limited to, policies and guidelines regarding sexual or other forms of harassment.

5.28 No e-mails may be sent externally outside of the Trust through the use of the automatic forwarding facility unless authorised. Staff must not use their personal email for work purposes.

5.29 Do not send large attachments unless absolutely necessary. Where drives are shared, indicate the location of the document in the e-mail so that the recipient can find the document. If you do send attachments you need to consider whether the document needs a copyright statement.

## **6.0 HOUSE KEEPING FOR E-MAL SYSTEMS**

6.1 Each mailbox has a storage limit and you must delete e-mail messages on a regular basis. If an important e-mail needs to be kept for future reference, save it in a personal folder.

6.2 If a Freedom of Information or Data Protection request is made all e-mails within your e-mail account could be shared if they are relevant to the request. Therefore ensure you delete your emails as soon as they are no longer needed ensuring that records management retention and destruction guidance is considered.

6.3 All email records destined for the internet will have an email disclaimer appended to the end of the email by the Trust systems. An example below details reference to the Freedom of Information Act 2000:-

*"The information contained in this email may be subject to public disclosure under the Freedom of Information Act 2000. Unless the information is legally exempt from disclosure, the confidentiality of this email, and your reply, cannot be guaranteed."*

## **7.0 SECURITY OF E-MAL**

7.1 When using the e-mail system, staff must be particularly aware of the following:

- vulnerability to unauthorised interception or modification;
- vulnerability to incorrect addressing;
- vulnerability to possible virus attachments;

7.2 Consideration should also be given to:

- the requirement to exclude sensitive information from the system;
- the exclusion of third parties from e-mail services.
- the use of NHS approved encryption techniques as they become available.

7.3 All staff will therefore comply with the following:

- treat e-mail as they would any other piece of correspondence, including appropriate language
- if the e-mail is regarding a patient/resident or staff member it should be printed off and filed in the person's record and then electronically deleted
- if an e-mail needs to be kept for other purposes, e.g. audit, it should be filed in the department's electronic system

## **8.0 CONTINUITY OF E-MAIL ACCOUNTS**

- 8.1 When staff are going on planned leave/absence from the workplace they should ensure that the 'Out of Office' tool is implemented to ensure e-mail communications are not disrupted and that any urgent communications can be redirected where necessary.
- 8.2 Some staff will, due to the nature of their roles, need to set up 'authorised' deputies to access e-mails on their behalf during periods of absence.
- 8.3 Deputies should not be provided with log on or user passwords for their colleagues but use the appropriate process for e-mails to be collected via their own log on credentials.
- 8.4 Where staff are absent due to unexpected leave requirement instructions should be provided using a Network Change Control form by the person's line manager and forwarded to the ITT Service Desk who will arrange for deputy status for the appropriate colleagues to be established.
- 8.5 When a member of staff is away from the office for an extended period, for example holiday/sick leave or after leaving the Trust, there may be occasions when it is necessary to access email messages from their account without express consent. The reasons for this access could be;
- Subject access request under the Data Protection Act/General Data Protection Regulation (GDPR)
  - Business Continuity (i.e. long term leave or illness)
  - Freedom of Information request
  - Evidence in legal proceedings
  - Evidence in a criminal investigation
  - Line of business enquiry
  - Evidence in support of disciplinary action
- 8.6 Access to a staff member's mailbox without expressed consent can only be authorised by a Director or the Head of IT&T.

## 9.0 USING INTERNET/INTRANET SYSTEMS

### **Acceptable Use:-**

- 9.1 The internet/intranet is to be used for work related purposes, for example to help with research for work, to access useful work related sites, for professional development and training or to obtain information related to work.
- 9.2 Any internet/intranet account provided by the Trust, assigned by the Trust to individuals, sub-units, or functions of the Trust, is the property of Essex Partnership University NHS Foundation Trust ('The Trust').
- 9.3 Those that use Trust internet/intranet services are expected to do so responsibly, that is, to comply with national laws, with this and other policies and procedures of the Trust, and with normal standards of professional and personal courtesy and conduct.
- 9.4 Access to Trust internet/intranet services, when provided, is a privilege that may be wholly or partly restricted by the Trust without prior notice when there is Substantiated Reason to believe that violations of law or policy have taken place, or, in exceptional cases, when required to meet time-dependant, critical operational need.
- 9.5 Access to internet/intranet will be inspected and/or monitored by Trust systems to protect the Trust, Trust Computing Facilities and account holders from internet/intranet borne viruses/macros/inappropriate attachments and/or content where possible.
- 9.6 The Trust shall permit the inspection, monitoring, or disclosure of internet access without the consent of the account holder of such sites which contain obscene, indecent, racist or illegal content:
  - when required by and consistent with law
  - when there is Substantiated Reason to believe that violations of law or of Trust Policies have taken place
  - when there are Compelling Circumstances
  - under time-dependent, critical operational circumstances as defined in the procedural guidelines (3.0).
- 9.7 It is understood that staff sometimes need to deal with personal / private matters during the working day. Limited personal use is therefore allowed provided it is kept to a reasonable level and does not interfere with the working day. This arrangement will be based on trust and all staff will be expected to use this facility in an appropriate manner. Staff should be aware that personal use of the internet will be monitored.

### **Unacceptable Use:-**

- 9.8 Staff are reminded that they are bound by confidentiality clauses in their contract of employment and should take extreme care about the content of information they share if using social networking sites. Reference to

contact with friends or other members of the public in the course of their work should be avoided to prevent potential breaches of confidentiality.

9.9 Access to the internet/intranet is provided for staff to use in the course of their work. Staff are prohibited to access, view, download, display or distribute any of the following:

- Content that expresses personal views about subjects unrelated to and inappropriate for a productive workplace;
- Accessing sites that relate to or provide information on criminal or terrorist activity; and/or
- Accessing sites that the whole prime function is to provide offensive materials. Posting, downloading or viewing pornography may constitute a criminal offence and is likely to be viewed as gross misconduct warranting summary dismissal.
- Anything which is otherwise offensive

9.10 Where staff inadvertently access websites which may fall into the group above (9.9) this should be reported to the Trust's ITT Helpdesk immediately.

9.11 Trust internet/intranet services may not be used for:

- unlawful activities
- commercial purposes not under the auspices of the Trust
- personal use that:
  - directly or indirectly interferes with the Trust operation of computing facilities, internet or email services
  - burdens the Trust with noticeable incremental cost
  - interferes with the user's employment or other obligations to the Trust
  - gives the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the Trust, unless appropriately authorised to do so.
  - employs false identity
- or uses that violate other Trust policies or guidelines
- the latter include, but are not limited to, policies and guidelines regarding sexual or other forms of harassment.

9.12 Staff must not use the internet, to attempt any unauthorised access to resources (hacking). Nor are staff allowed to access hacker websites as some sites contain traps which may trigger malicious programmes when a page is read.

#### ***Joining Chat Rooms and News Groups:-***

9.13 Staff may join a chat group or news group related to work. Staff are required to conduct themselves in a professional manner, be courteous and inoffensive. Unless you are authorised to do so, staff are not permitted to write or present views on behalf of the Trust or any NHS organisation. Some groups may require permission to be granted for access. Under no circumstances should patients be identified during discussions.

*(Refer to the Social Media Policy/Procedure for further guidance.)*

## **10.0 OBTAINING E-MAIL ACCESS**

- 10.1 Where an e-mail account has not been provided to an individual at the stage when their network account has been set up, the line manager must make a request to the relevant ICT service provider using the appropriate approval route.
- 10.2 The IT&T Department will install software to enable staff to access the Trust e-mail facilities. The software must not be reconfigured by members of staff, other than those in the IT&T Department.
- 10.3 Only software provided by the Trust's IT&T Department may be used to access e-mail facilities.

## **11.0 MONITORING INTERNET/INTRANET/E-MAIL SYSTEMS**

- 11.1 A username and password restrict the use of internet/intranet/e-mail services. All use of the system is logged against the username and the Trust will assume that this is the authorised person accessing the facilities.
- 11.2 Trust staff must not share usernames or passwords with colleagues.
- 11.3 In the event of abuse/misuse of the Trust's internet/intranet/e-mail services all access will immediately be revoked pending any investigations and staff may be investigated through the Trust's disciplinary procedures in the event that abuse of internet/intranet/e-mail services is proven.
- 11.4 The automated monitoring software used provides an audit trail of the addressee, recipient and contents of the e-mail. We reserve the right to monitor your use of e-mail at any time for operational reasons and to review, monitor, replicate, audit and disclose any material held on any IT system, including laptops owned by the organisation, to investigate and guard against the misuse of e-mail. If a breach of e-mail use is detected, a full enquiry will be undertaken. Disciplinary procedures may be started which may ultimately lead to dismissal or criminal prosecution. Serious offences, even for the first time, may constitute gross misconduct justifying summary dismissal.
- 11.5 The automated monitoring software used provides an audit trail of who logged on to an internet site, when, for how long, which sites were accessed, number of attempts to access sites and whether a file transfer took place. Offensive site access is tracked and excessive use of the internet is flagged up. Staff need to bear in mind that some sites track the unique address for your computer (IP-address) so they can track you or the organisation you work for. We reserve the right to monitor your use of the internet/intranet at any time for operational reasons and to review, monitor, replicate, audit and disclose any material held on any IT system, including laptops owned by the organisation, to investigate and guard against the

misuse of internet/intranet access. If a breach of internet/intranet access is detected, a full enquiry will be undertaken. Disciplinary procedures may be started which may ultimately lead to dismissal or criminal prosecution. Serious offences, even for the first time, may constitute gross misconduct justifying summary dismissal.

**END**

SAMPLE ONLY

## INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

<b>POLICY REFERENCE NUMBER:</b>	CPG50d	
<b>VERSION NUMBER:</b>	3	
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	3 year review; minor changes	
<b>AUTHOR:</b>	[REDACTED] Information Governance Manager	
<b>CONSULTATION GROUPS:</b>	Information Governance Steering Sub-Committee. Quality Committee.	
<b>IMPLEMENTATION DATE</b>	June 2019	
<b>AMENDMENT DATE(S)</b>	October 2019 (ID no. Change); Sept 2021	
<b>LAST REVIEW DATE</b>	September 2021	
<b>NEXT REVIEW DATE</b>	September 2024	
<b>APPROVAL BY IGSSC</b>	August 2021	
<b>RATIFICATION BY QUALITY COMMITTEE</b>	September 2021	
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2019-20221. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner	
<b>PROCEDURE SUMMARY</b>		
<p>The purpose of this policy and its associated procedural guidelines is to establish the governance arrangements and responsibilities for information security, with the intention to promote and build a level of consistency across the Essex Partnership University NHS Foundation Trust ('the Trust') to safeguard information, ensuring all Trust staff are aware of their individual responsibilities.</p>		
<b>The Trust monitors the implementation of and compliance with this procedure in the following ways:</b>		
<p>The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Information Service Management Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this policy and its associated procedures, as appropriate. Also through Trust Datix Reporting and Compliance with the IG Toolkit submission</p>		
<b>Services</b>	<b>Applicable</b>	<b>Comments</b>
Trustwide	✓	

**The Director responsible for monitoring and reviewing this policy is  
The Executive Chief Finance & Resources Officer**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**INFORMATION GOVERNANCE INCIDENT  
REPORTING PROCEDURE**

**CONTENTS**

THIS IS AN INTERACTIVE CONTENTS LIST – PLEASE CLICK ON THE SECTION HEADINGS TO GO TO THE SECTIONS

**1.0 INTRODUCTION**

**2.0 PURPOSE**

**3.0 DEFINITIONS**

**4.0 ROLES AND RESPONSIBILITIES**

**5.0 REPORTING PROCESS**

**6.0 STAFF, PATIENT AND CARERS SUPPORT**

**7.0 UNDERTAKING AN INVESTIGATION**

**8.0 MISCONDUCT**

**9.0 GRADING INCIDENTS**

**10.0 ANALYSIS AND FEEDBACK OF COLLATED REPORTS**

**APPENDICES**

**APPENDIX 1 – SECURITY INCIDENT OPENING REPORT FORM**

**APPENDIX 2 – INFORMATION SECURITY INCIDENT INVESTIGATION FORM**

**APPENDIX 3 - INFORMATION SECURITY INCIDENT REPORTING PROCESS**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE**

**1. INTRODUCTION**

- 1.1 This procedure is a Trust-wide document and applies to all staff.
- 1.2 It should be read in conjunction with the Trust's Information Security Incident Management Procedure & Risk Management Policy.
- 1.3 The Trust is committed to the promotion of a learning and fair blame culture, where staff understand the need to report all incidents.
- 1.4 Throughout this policy an incident refers to all accidents, incidents and near misses.
- 1.5 All Trust staff should report any incident including near misses, incidents and safety issues. The Trust assures staff through processes such as the 'whistleblowing policy' (Raising Concerns (Whistleblowing Policy, CP53) that the information they share will be treated with respect and acted upon appropriately to improve the safety and quality of the service we provide for our patient/service users and the safety and quality of the work environment for staff and visitors.
- 1.6 In line with the Duty of Candour Requirements (2014) the Trust also has a Being Open policy (CP36) to ensure that when mistakes are made patients/relatives/carers receive an acknowledgement, apology and a truthful and clear explanation as soon as a patient safety incident has occurred.

Saying sorry is not an admission of liability it is the right thing to do.

- 1.7 Communication with patients, carers and the public must be fully documented.

**2. PURPOSE**

- 2.1 The aim of the procedure is to provide:
  - Staff with clear information on how to report incidents via the Datix electronic online incident reporting system
  - An outline of the management of incident reporting in the Trust and to external agencies/stakeholders
  - The Trust's approach on the investigation, analysis, and learning and improvement from incidents
  - A procedure for the investigation of reported as major or catastrophic harm including SIRIs (Serious incidents requiring investigation) Near Miss and Never Events.

## CPG50D – Information Governance Incident Reporting Procedure

- Procedures for investigating specific generic incident types
- 2.2 The purpose of the procedure is to outline the arrangements for identifying, managing, investigating and reporting accidents, incidents and near misses within the Trust.
- 2.3 This procedure covers reporting and recording procedures for managers, employees and non-employees.
- 2.4 The reporting of all incidents, prevented incidents (near-misses) is designed to ensure the following:
- A culture of openness in reporting incidents or prevented incidents (near misses);
  - Prompt and precise gathering of information;
  - Prompt communication with staff and where appropriate the media;
  - Minimisation of distress to those affected by an incident;
  - Identification of patterns and trends in the occurrence of incidents and prevented incidents (near-misses);
  - Minimise, so far as is reasonably practicable, future risk by taking prompt and appropriate preventive action and on - going monitoring;
  - Early warning of potential litigation and cost impact;
  - Managers are able to review existing safety procedures;
  - Fulfilment of the Trust's legal duties under statutory regulations.

### 3. DEFINITIONS

For the purposes of this procedure the following definitions apply:

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy

## CPG50D – Information Governance Incident Reporting Procedure

- Other significant economic or social disadvantage to individuals

### 4. ROLES AND RESPONSIBILITIES

#### Duties within the Organisation

##### 4.1 Executive and Senior Team

Executives and senior managers are responsible for the health and safety of employees and visitors in their specified location/areas. As such they have the primary responsibility for ensuring this procedure is fully implemented in their area.

##### 4.2 Managers

Managers are responsible for implementing the policy by:

- Ensuring that all staff are up to date with Information Governance training aware of the procedures;
- Support & encourage staff in the reporting of accidents and near misses;
- Ensuring appropriate and timely reporting of incidents;
- Supporting the reporting process of reviewing and investigating local incidents;
- Taking local remedial and preventative action;

##### 4.3 Employees

All employees are responsible for:

- Reporting any incident/accident/near miss in line with this procedure;
- Adhering to the employee requirements of the Health & Safety at Work Act 1974;
- Provision of reports as requested as part of an investigation.
- Undertake the annual mandatory training

### 5. REPORTING PROCESS

5.1 All incidents (including near misses and out of hours) must be reported using the Trust reporting electronic system called Datix. Datix provides a systematic process which enables incidents to be reported and then investigated.

5.2 All incidents should be reported as soon as the staff member is able, ideally within 24 hours ensuring patient safety remains a priority.

Do not delay reporting if some information is unavailable; this can be added later.

5.3 All staff have access to Datix. Datix is found on the Staff Input pages.

## CPG50D – Information Governance Incident Reporting Procedure

- 5.4 For all patient safety incidents reported as moderate, major or catastrophic harm, the Trust has a 'Duty of Candour' to offer an apology to the patient or relevant person.
- 5.5 Datix electronic incident reporting forms must be completed as comprehensively as possible and should give a clear factual and objective account of what happened i.e. who, why, what, where and how. They should also include information on the immediate actions taken following the incident together with any actions planned or taken to prevent a reoccurrence.
- 5.6 Incident forms must contain factual information and exclude personal opinion or assumption.
- 5.7 If an incident has involved a patient, clinical staff must also record what happened and any action taken in the patient's medical records.
- 5.8 Notifiable breaches are those that are likely to result in a high risk to the rights and freedoms of the individual (data subject). The scoring matrix used in incident reporting has been designed to identify those breaches that meet the threshold for notification.
- 5.9 However, there are also a number of breaches of security that are also reportable under Network and Information Systems Regulations 2018 which must also be recorded on the Data Security & Protection Tool even if organisations believe they are not notifiable under the General Data Protection Regulation (GDPR).
- 5.10 The GDPR Article 33 requires reporting of a breach within 72 hours. The 72 hours starts when an organisation becomes aware of the breach which may not necessarily be when it occurred. An organisation must have a reasonable degree of certainty that a security incident has occurred and that this has led to personal data being compromised.
- 5.11 This means that once a member of staff or the public has reported a breach this is the point that an organisation is aware. The actual incident may have occurred some hours, days or weeks previously, but it is only when an organisation is aware that the breach has occurred that the 72 hours to notification period starts.
- 5.12 Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

### **5.13 Local records required for an incident notified to the ICO**

A local file, which may be requested by the Information Commissioner, must be maintained which must contain the following sections;

- the facts relating to the breach.
- its effects.
- the remedial action taken.

## CPG50D – Information Governance Incident Reporting Procedure

The local file of the investigation for the Trust is the Datix System.

The Datix reporting tool will forward to the appropriate organisation indicated in the scoring matrix. The organisations may have obligations to work with other agencies, such as the National Cyber Security Centre, for example, and any incident may be shared onward.

### 5.14 ICO

Any incident graded as notifiable, will be reported by the Information Governance team through the Data Security & Protection Toolkit (DSPT) to the ICO and will result in the incident being forwarded to the Information Commissioner. The Information Commissioner will then decide if any action is necessary.

### 5.15 Department of Health and Social Care

Any incident that scores more than a 3 on both axes on the scale will be immediately reported to the Department of Health and Social Care so that the relevant officials can be made aware of any breach that is likely to have an impact on service users and the running of the health and social care sector.

### 5.16 NHS England

Any incident that scores more than a 3 on both axes on the scale will be reported to NHS England to help inform operational delivery and future commissioning arrangements.

### 5.17 NHS Digital

As well as hosting the Data Security and Protection Incident Reporting Tool the information contained within reported breaches may be used as intelligence especially when there could be an effect on the system and services it provides which are relied upon across the sector.

## 6. STAFF, PATIENTS AND CARERS

Involvement in an incident can undermine confidence for patients, carers and families. The member of staff who is nominated to inform the patient/relative/carer about the incident should offer all necessary support. [Trust's Being Open Policy]

Staff who are responsible or involved in an incident should receive feedback, from their manager, regarding any investigation, including recommendations and actions taken to reduce the risk of reoccurrence.

## 7. UNDERTAKING AN INVESTIGATION

- 7.1 The individual to whom the incident has been assigned (the handler) should ensure an investigation occurs.

The Handler must record the details of the investigation and the outcome on Datix.

This person remains responsible for ensuring that all relevant information is documented on the online Datix investigation form and that sufficient information is provided on the feedback section of the form.

- 7.2 Investigations should be carried out in such a way as to promote a non-threatening environment, with emphasis on learning from the incident, rather than apportioning blame.

- 7.3 Confidentiality of all individuals concerned should be protected as far as possible throughout the investigation, ensuring all written documentation is stored in a secure environment.

- 7.4 An investigation must be carried out as soon as possible after an incident has occurred.

A good starting point is to collate and gather initial evidence, for example by speaking with staff, visiting the scene, collecting any relevant documentation and securing any evidence.

Additional information that may need to be obtained includes for example, training records, risk assessments, staff duty rotas, policies and procedures, etc.

- 7.5 All details regarding the incident must be documented and all staff should be reminded that any records kept may be disclosable.

The information gathered should be reviewed, a chronology of events determined and the following key pieces of information established:

- What happened? Where? Check exact locations and times.
- Who was involved?
- Who was affected?
- Has it happened before?
- What impact has the incident had?
- Were there any witnesses?
- What action has already been taken? By who?
- Who has been informed?
- Has an incident form been submitted?
- Do written statements need to be obtained?
- Who else needs to know? e.g. external agencies/stakeholders and/or internal departments/key individuals
- What else needs to be done?

## CPG50D – Information Governance Incident Reporting Procedure

- 7.6 Some investigations will require staff to provide written statements of their involvement. This can best be achieved by contacting the individual and making a record of their description of events.

### 8. MISCONDUCT

- 8.1 Where an incident upon investigation, identifies that an individual acted in a manner, which knowingly placed themselves and others at significant risk or if misconduct or fraudulent behaviour is identified, disciplinary action may follow.
- 8.2 If a member of staff knowingly fails to report an incident it will be in breach of this procedure.
- 8.3 Where an individual staff member repeatedly make the same mistakes, or are persistently closely involved with incidents and fail to learn from the support and training provided by the organisation, then the Trust's Capability policy and procedures will be followed.

### 9. GRADING INCIDENTS

- 9.1 The severity of an incident or consequence, along with the likelihood of reoccurrence is applied to the incident which could involve staff, patients and others to establish a grade e.g. near miss, negligible, minor, moderate, major, and catastrophic.

A scoring matrix (below) is used by the Information Governance team to help identify the appropriate score for an incident.

All incidents including near misses are graded; however a near miss will be graded in relation to the potential harm as opposed to the actual harm.

#### 9.2 Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of special categories/vulnerable groups it must be assessed as at least:

- A Likelihood of 'Not likely or incident involved vulnerable groups (where no adverse effect occurred)' Not Likely on the grid.

And

- A Severity of 'Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred'. Minor on the grid.

So even where an incident involves special categories/vulnerable groups, on the breach assessment grid above, it would be a minimum of 4 and so would not be always be reported to the ICO. It would be reported to the ICO if the Likelihood of harm is assessed as at least 'Likely'.

## CPG50D – Information Governance Incident Reporting Procedure

### 9.3 Special Categories of personal data

For clarity special categories under GDPR are:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- the processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation

### 9.4 For clarity special categories under GDPR not listed above include:

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010  
(where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual)
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

### 9.5 Assessing risk to the rights and freedoms of a data subject (likelihood) The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Depending on the outcome of the scoring matrix contained in this procedure the risk may be high risk and be significant enough to notify to the ICO. If there is any doubt that a breach is significant enough for notification it is always best to notify.

## CPG50D – Information Governance Incident Reporting Procedure

### 9.6 Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “grey breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

## 10. ANALYSIS AND FEEDBACK OF COLLATED INCIDENT REPORTS

10.1 The Trust recognises the importance of learning. In order to ensure an aggregated review of incidents and the opportunity to learn wider lessons, the Associate Director of Electronic Systems and Information Governance will be responsible for co-ordinating a monthly report to the Learning Oversight sub-committee (LOSC) meeting.

10.2 Escalating concerns/issues identified through analysis

The LOSC meeting will escalate any unresolved issues to the Trust Quality Committee. The Quality Committee will receive assurance that work streams are progressing.

10.3 Incidents should be discussed at Ward/Department meetings. Amber and Red incidents will be discussed at the Information Governance Steering Group / Quality Board. The identified actions and lessons learned are shared Trustwide in the staff Wednesday Weekly Communication Articles.

**END**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONTRACT FOR PROVIDING A STAFF WORK MOBILE PHONE NUMBER TO A  
PATIENT / CARER

Patient's Name.....

Staff Member's  
Name.....

Staff Work Mobile  
Number.....

Trust Emergency Contact Number.....

This mobile phone number has been provided for the following uses:

.....  
.....  
.....

This number must not be used in cases of emergency.

Messages can / cannot be left  
Any messages left will be addressed during the hours of .....

I agreed to abide by the above conditions

Signed.....

Designation.....  
(On behalf of the MDT)

Date.....

Signed.....

(Patient/Carer\*)  
\* delete as appropriate

Date.....

**SAMPLE - DO NOT USE**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONTRACT FOR PATIENT USE OF A MOBILE TELEPHONE

Patient's Name.....

Ward / Nursing Home/ Residential Area.....

**Risk Assessment**

Is the mobile phone a camera phone which would affect levels of privacy and dignity?

Is the mobile phone capable of audio recording?

Does this mobile phone have email or internet capabilities?

**If Yes to any of these, consent is required from the patient that they will not use the phone for these purposes.**

Would use represent a threat to patients' own safety or that of others?

**If Yes, use must be denied**

Are there any electrically sensitive medical devices that would be affected?

**If Yes, use must be denied**

The above patient has been granted the use of a mobile telephone subject to the following conditions:

- 1 That the telephone will only be used within the designated agreed area
- 2 That the mobile phone will only be used for the purpose of conversations and texts.
- 3 That the mobile phone is not charged in any patient area
- 4 That the mobile phone is used subject to any other conditions required by the multidisciplinary team / clinical team
- 5 That my mobile phone may be removed if conditions are not abided by

The other conditions are:

.....  
.....

I agreed to abide by the above conditions

Signed.....

Signed.....

(Patient)

Designation.....

(On behalf of the MDT)

Date.....

Date.....

## USE OF MOBILE PHONES PROCEDURE

<b>PROCEDURE REFERENCE NUMBER:</b>	CPG54
<b>VERSION NUMBER:</b>	2
<b>KEY CHANGES FROM PREVIOUS VERSION</b>	EPUT Format
<b>AUTHOR:</b>	██████████ Advancing Clinical Practice Lead
<b>CONSULTATION GROUPS:</b>	Trust wide: Operational Managers Estates & Facilities  Compliance & Risk Team Mobius / Paris Team Pharmacy
<b>IMPLEMENTATION DATE:</b>	April 2017
<b>AMENDMENT DATE(S):</b>	February 2020
<b>LAST REVIEW DATE:</b>	April 2020
<b>NEXT REVIEW DATE:</b>	April 2023
<b>APPROVAL BY CLINICAL GOVERNANCE &amp; QUALITY SUB-COMMITTEE:</b>	February 2020
<b>RATIFICATION BY QUALITY COMMITTEE:</b>	April 2020
<b>COPYRIGHT</b>	© Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be produced in whole or in part with the permission of the copyright owner.

PROCEDURE SUMMARY		
<p>The purpose of this procedure is to identify working arrangements for the use of Mobile Phones within all areas of the Trust for Staff, Patients and Visitors. The widest possible use of mobile phones for Staff, Patients and Visitors will be considered within patient areas: where local risk assessments indicate that such use would not represent a threat to patients' or others own safety and security. Risk Assessments must include use of the operation of electronically sensitive medical devices in critical care situations or where levels of privacy and dignity may be affected. 'Patient' will be the terminology used throughout this document and will refer to a patient, resident or service user.</p>		
The Trust monitors the implementation of and compliance with this procedure in the following ways;		
<p>Auditing for compliance will be undertaken a minimum of 3 yearly by operational managers/leads and the results presented to the appropriate Trust Committee for consideration.</p>		
Services	Applicable	Comments
Trustwide	✓	
Essex MH&LD		
CHS		

**The Director responsible for monitoring and reviewing this procedure is  
Executive Director of Nursing**

**ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST**

**PROCEDURAL GUIDELINES ON THE USE OF MOBILE PHONES**

**CONTENTS**

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

- 1.0 INTRODUCTION
- 2.0 SCOPE
- 3.0 DESIGNATED MOBILE PHONE USE AREAS
- 4.0 STAFF USE OF MOBILE PHONES
- 5.0 PATIENT USE IN INPATIENT, DAY AND RESOURCE CENTRE AREAS
- 6.0 PRECAUTIONARY MEASURES
- 7.0 MOBILE PHONE CHARGERS
- 8.0 REPORTING BREACHES
- 9.0 MONITORING & REVIEW
- 10.0 REFERENCES

**APPENDICES**

**APPENDIX 1 – CONTRACT FOR PROVIDING A MOBILE PHONE NUMBER TO PATIENT / CARER**

**APPENDIX 2 – CONTRACT FOR PATIENT USE OF A MOBILE TELEPHONE**

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROCEDURAL GUIDELINES ON THE USE OF MOBILE PHONES

1.0 INTRODUCTION

- 1.1 Whenever anyone is in hospital/Nursing Home or within a residential community, day or resource centre setting, communication with family and friends may become an essential element of support and comfort, the widespread use of mobile phones and their integrated functionality such as texting and e-mailing may provide a positive aspect of support.
- 1.2 Mobile phones may have extended functions which include camera, audio and video recording capability, music players, email and internet functions. There is a potential for patients and visitors to use this functionality to take inappropriate photographs, videos or recordings that present potential to interfere with patient dignity and privacy.
- 1.3 In 2016 NHS Protect which was replaced by NHS Counter Fraud Authority in 2017, produced good practice advice in their "Patients Recording NHS staff in Health and Social Care Settings" May 2016 document for use in health and social care settings. The document provides clarification to NHS clinical and non-clinical staff working within health and social care settings on dealing with situations where patients might record their treatment and care. This advice covers both covert and overt recording of consultations. However, it predominantly concerns overt recording as the patient will generally ask NHS staff for permission for recording to take place.
- 1.4 There are no specific legal requirements that govern an individual making a personal recording of their medical consultation or treatment, either overtly or covertly, for their private use. The position may, however, change once a recording is no longer used as a record of the consultation, for example where the recording is disclosed or publicised in a modified way which is not connected to the consultation. This could include an instance where it is designed to cause detriment to or harass another individual captured in the recording. Any such disclosure or publication, depending on the nature and context, may attract a civil action for damages and may also be a criminal offence which **could include an offence contrary to section 1 of the Protection From Harassment Act 1997, an offence contrary to section 4, 4A or 5 of the Public Order Act 1986, an offence contrary to section 1 of the Malicious Communications Act 1988 or an offence contrary to section 127 of the Communications Act 2003.**
- 1.5 In addition, ring tones or music played via mobile phones could disturb others who are trying to recuperate and constant 'chatter' of other patients, visitors or staff on mobile phones may be equally disruptive to those patients wishing to rest. Mobile phones could also potentially interfere with medical equipment and affect their use.

- 1.6 The Trust has designated mobile phone use areas, these are the only areas in which the use of mobile phones is permitted without a risk assessment being completed.

## **2.0 SCOPE**

- 2.1 This procedure applies to all Staff, Patients and Visitors in all areas of the Trust.

## **3.0 DESIGNATED MOBILE PHONE USE AREAS**

### **3.1 Designated Areas**

- 3.1.1 Non patient areas are defined as those areas where there is no patient access.
- 3.1.2 Non patient areas and Trust reception areas are designated as acceptable for mobile phone use, where issues of privacy and dignity and interference with medical equipment can be kept to a minimum.
- 3.1.3 Reception areas are defined as areas where patients and visitors have unlimited access and which are staffed at all times (this does not include ward reception areas).
- 3.1.4 For all other areas, risk assessments must be undertaken to assess whether the use of mobile phones is appropriate. In these areas a sign should be displayed at the area entrance which directs staff, patients and visitors to contact the unit/department/home manager to confirm whether or not mobile phone use is allowed.
- 3.1.5 The possession or use of mobile phones is strictly prohibited to all staff, patients, contractors and visitors entering clinical areas at Brockfield House, Robin Pinto Unit, Woodlea Clinic, Hadleigh Unit, Edward House, Christopher Unit, Larkwood ward. When entering patient areas in these units mobile phones should either be left in staff vehicle, at home or placed in the lockers within the reception area. However, where someone needs use of a mobile phone for work related tasks then permission must be requested via security or in their absence one of the integrated clinical leads/unit coordinator for their authority. For all other not working on any of the secure wards at Brockfield, Robin Pinto, Woodlea Clinic, Hadleigh Unit, Edward House, Christopher Unit and Larkwood ward will now be able to bring their mobile phone into non patient areas only. Staff in Larkwood ward and on Poplar Unit in Rochford must read this procedure in conjunction with the Unit's protocols on the use of Mobile phones.

### **3.2 Risk Assessments**

- 3.2.1 Some patient areas can also be designated as a mobile phone use area. Local Risk Assessments must be undertaken to determine if a patient area is to be designated as a mobile phone use area, using the Trust General Workplace Risk Assessment Form (RM11 Appendix 2) which is on intranet.

- 3.2.2 Any local area designated as a mobile phone use area must be outlined in local Operational Policies.
- 3.2.3 Camera functions, audio or video record functions may not be used in any Trust area. The only exception to this is for staff and teams where a job role or function demands this use and they must seek permission from a senior manager.
- 3.2.4 Any staff member who witnesses the use of such functions must ask the offender to stop, inform a senior manager, complete a Datix incident form and if the offender is a patient, inform their care coordinator or named nurse (where appropriate).
- 3.2.5 The use of camera phones within patient areas or patient's own home risks breaching patient confidentiality. The only exception to this is for staff where a job role or function demands this use for example in community health services staff take photographs of wounds to monitor healing and the Risk Team when conducting inspections and incident follow up work.
- 3.2.6 Patients and Visitors will be made aware of the Trust procedures concerning the use of mobile phones within the patient areas through information leaflets and local posters.

#### **4.0 STAFF USE OF MOBILE PHONES**

##### **4.1 General Use**

- 4.1.1 Secure services have their own mobile phone operational protocols therefore staff, patients and visitors in these services must refer to Use of Mobile Telephone within Secure Services Protocols.SSOP35 and SSOP40 which are on intranet.
- 4.1.2 For all other services staff on duty may use mobile phones for work related issues within mobile phone use designated areas. Staff may also use mobile phones within patient areas, where a local risk assessment has been undertaken, however, consideration must be given to patients who are resting and only in emergency circumstances should a mobile phone be used within earshot of a patient. Staff can use mobile phones for personal use only when on designated breaks except for emergency use as detailed in section 4.1.5 below.
- 4.1.3 All Trust employees must adhere to the law in relation to the use of mobile telephones whilst driving. With effect from December 2003 the hand-held use by a driver of a mobile phone in a car is in direct breach of road traffic regulations. In no circumstances must a mobile phone be used when driving, unless using 'hands-free' equipment. In such circumstances, it is the driver's responsibility to ensure it is safe to make or receive calls, given the driving conditions at the time. They must:-
- Keep calls as short as possible,
  - Avoid complex or emotionally sensitive calls,

- Never hold the phone or send or read a text message.

In general, drivers must endeavour to stop in a safe place to make or receive calls.

- 4.1.4 Staff may not use the camera function, any of the recording functions, or play music within patient areas, unless this falls within their job role to do so.
- 4.1.5 Staff are reminded that the use of mobile phones must be kept to a minimum and for emergency use only. Whilst it is appreciated that family and friends may need to contact you, or you them, under special circumstances (e.g. illness) the use of mobile phones must not in any way impact on the workplace (e.g. workload, distraction to team members, putting private calls before business calls, during engaging and observation of patients).
- 4.1.6 Where special circumstances occur members of staff must liaise with their line management to apprise them of the situation.
- 4.1.7 If a staff member uses their phone inappropriately this will be addressed by their manager through the Conduct & Capability Policy and Procedure HRPG27a.
- 4.1.8 If a mobile phone is lost or stolen the phone user will complete a Datix incident reporting form and advise IT and Purchasing department so the phone can be barred. (Guidance on completing this form can be found in the Trust's Adverse Incident Procedural Guidelines CPG3).

## **4.2 Clinical Use**

- 4.2.1 Secure services have their own mobile phone operational protocols therefore staff in these services must refer to secure services mobile phone protocols which are on intranet.
- 4.2.2 Where possible staff are encouraged not to give out individual telephone numbers.
- 4.2.3 If in any circumstances, it is felt necessary for staff to provide a patient or carer with their work mobile phone number and not personal, they must undertake a risk assessment. The assessment must take into consideration how the staff member will ensure that this work number is not used in place of an emergency number and how the staff member will ensure that it is answered even when not on duty.
- 4.2.4 Both the staff member and the patient or carer must agree the conditions for use of their work mobile phone number using the contract for providing a staff work mobile phone number to a patient / carers (Appendix 1).
- 4.2.5 If it is necessary to provide a work contact number the contact centre number must be used or a locally agreed out of hours number. Hours of contact must be made clear to patients/carers and staff as well as

any alternative arrangements and any specific agreements documented in their care plan. The contact centre number is **0300 123 0808**. They provide a messaging service within agreed working hours and will hold all teams contact numbers that connect patients to staff.

#### **4.3 Text Messaging**

- 4.3.1 Any text message sent to or received from a patient, carer or colleague is classified as patient information and must be treated with the same rules around confidentiality as any other patient information / record.
- 4.3.2 All text messages sent to or received from patient or carers must be recorded in the patient notes.
- 4.3.3 The use of text messaging must be risk assessed before being undertaken.

#### **5.0 PATIENT USE IN INPATIENT / NURSING HOME, DAY AND RESOURCE CENTRE AREAS**

- 5.1 Secure services have their own mobile phone operational protocols therefore, staff in these services must refer to secure services mobile phone protocols which are on intranet.
- 5.2 On admission to inpatient ward, Day Treatment services and Resource centers patients must be made aware of the Precautionary Measures in 6.0 on page 8 of this document.
- 5.3 Any mobile phone retained for use by the patient must be used in a designated Trust or locally risk assessed area under agreed conditions.
- 5.4 A copy of the Risk Assessment and the Contract for Patient Use of a Mobile Phone (appendix 2) must be completed and signed by the patient and a member of the Multi-Disciplinary Team (MDT)/Clinical team. Both must be kept within the patients notes.
- 5.5 Risk Assessments for patient use of a mobile phone must include an assessment of the following for individual patient use:
  - Whether the mobile phone is a camera phone
  - Whether the mobile phone has email or internet functionality
  - If the mobile phone is capable of audio / video recording
  - The management and use of charging leads/wires
  - Whether use would represent a threat to patients' own safety or that of others
  - Whether the operation of electrically sensitive medical devices in critical care situations would be affected
  - Whether levels of privacy and dignity would be potentially affected
- 5.6 Extended functions, on any mobile phone cannot be used on Trust premises. Please see below

- 5.7 If it is assessed that a person continually abuses a mobile phone the issue will be re-assessed by the MDT/Clinical team regarding individual use and potentially removed. However, staff will ensure that patient have access to a phone if required e.g. ward phone. In any situation where the staff member in charge considers a breach of confidentiality or potential breach of confidentiality mobile phone use must be reassessed as soon as possible. Any breach of confidentiality must be reported using guidelines as set out in Adverse Incident and Serious Untoward Incidents Policy CP3
- 5.8 Any mobile phone brought in to the inpatient area which is assessed and not agreed for the patient to use will be retained by staff for safekeeping using Trust Policy regarding property (Patient/Client Property and Money Procedure FP09/02) or will be returned home with agreement from the Patient to a relative or friend.

## **6.0 PRECAUTIONARY MEASURES**

### **6.1 Overt patient recordings**

Although we cannot place restrictions on a patient wishing to record notes of a consultation or conversation with a health professional, where it is felt absolutely necessary by the patient to do so, staff should ensure that:

- Any recording is done openly and honestly.
- The recording process itself does not interfere with the consultation process or the treatment or care being administered.
- The patient understands that a note will be made in their health record stating that they have recorded the consultation or care being provided.
- The patient is reminded of the private and confidential nature of the recording and that it is their responsibility to keep it safe and secure.
- Any recording is only made for personal use.

### **6.2 Covert patient recordings**

Although we cannot place restrictions on a patient wishing to covertly record a consultation or conversation with a health professional, where staff are aware that covert recording has occurred they should ensure that:

- The issue is discussed with the patient as per 6.1 above.
- Relevant staff should consider providing patients with a written record summary, and or a verbatim record (if practical) of their consultation for their own personal use
- Patients are advised that they are entitled to see their notes, if they so wish, by informally asking the healthcare professional in charge of the consultation, or to request a paper copy of their medical notes formally through a Subject Access Request (SAR) made under the Data Protection Act 2018.

Patients are given information on how they can complain if they have an issue with their treatment and care, and their attention is drawn to the relevant guidance from the Care Quality Commission (see below) and Information Commissioner's Office.

## **7.0 MOBILE PHONE CHARGERS**

- 7.1 Mobile phones need to be charged via the mains power supply, consequently there may be a ligature / other health and safety risks involving wires. All patient areas must risk assess this activity before mobile phone chargers are used.
- 7.2 Only approved chargers compatible with the make and model of the phone may be used when charging mobile phones on Trust premises. Whether Trust or personal property, the charger must be up to date in relation to portable appliance testing (PAT) before permitted for use. Failure to observe this requirement will contravene Health and Safety Regulations and could place individuals at risk.
- 7.3 To avoid probability or likelihood of leaving devices unplugged medical devices are not to be unplugged to charge phone.
- 7.4 Recent information has also been identified regarding the potential danger of using an electrical device whilst still attached to the mains electricity supply, therefore, mobile phones must not be used whilst still plugged in to the mains electrical supply.

## **8.0 REPORTING BREACHES**

8.1 Any staff member who witnesses the use of video or audio recording which has not been agreed by all concerned must:

- ask the individual to stop
- inform a senior manager
- inform Information Governance leads via completion of a Datix incident form

If the individual is a patient complete Datix incident form and inform also their doctor, named nurse and care co-ordinator (where appropriate).

## **9.0 MONITORING AND REVIEW**

- 9.1 This policy and procedural guideline will be reviewed and monitored for compliance 3 yearly or as required by legislation/best practice guidelines.
- 9.2 Auditing for compliance will be undertaken a minimum of 3 yearly by operational managers/leads and the results presented to the appropriate Trust committee for consideration.
- 9.3 Following an incident where a mobile phone interferes with medical equipment this must be reported on Datix. The Integrated Risk Team will then be responsible for reporting this to the MHRA and NPSA as required.

## **10.0 REFERENCES**

- NHS Protect, Patients recording NHS staff in health and social care settings (March 2016)
- [http://www.cqc.org.uk/sites/default/files/20150212\\_public\\_surveillance\\_leaflet\\_final.pdf](http://www.cqc.org.uk/sites/default/files/20150212_public_surveillance_leaflet_final.pdf)
- Department of Health, 'Using mobile phones in NHS hospitals', (2009)

- [http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod\\_consum\\_dh/groups/dh\\_digitalassets/@dh/@en/documents/digitalasset/dh\\_092812.pdf](http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_092812.pdf)
- NHS Protect – Misuse of Social Media to Harass, Intimidate or Threaten NHS Staff May 2016.

END

SAMPLE - DO NOT USE