NHS
Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE AND SECURITY POLICY

POLICY REFERENCE NUMBER:	CP50
VERSION NUMBER:	3.1
KEY CHANGES FROM PREVIOUS VERSION	3 year review
AUTHOR:	Alice Williams Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub-Committee. Quality Committee.
IMPLEMENTATION DATE	May 2018
AMENDMENT DATE(S)	Feb 2018; May 18 (GDPR); May 2021; April 2022
LAST REVIEW DATE	May 2021
NEXT REVIEW DATE	May 2024
APPROVAL BY IGSSC	April 2021
RATIFIED BY QUALITY COMMITTEE	May 2021
COPYRIGHT	

PROCEDURE SUMMARY		
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.		
The Trust monitors the implementation of and compliance with this procedure in the following ways:		
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 & Protection Toolkit submission		
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

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

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
- Acceptable 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 Sub-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 place 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 necessary 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 31st 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 – Acceptable 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 – Cyber Incident Response Procedure v4
CPG50I – Cyber Incident Response Plan

END

Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE & SECURITY PROCEDURE

PROCEDURE NUMBER:	CPG50
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	3 year review; Minor amendments
AUTHOR:	Information Governance Team
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE	April 2017
AMENDMENT DATE(S)	July 2018; September 2021
LAST REVIEW DATE	September 2021
NEXT REVIEW DATE	September 2024
APPROVAL BY IGSSC	August 2021
RATIFIED BY QUALITY COMMITTEE	September 2021
COPYRIGHT	

PROCEDURE SUMMARY

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.

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.

The Trust monitors the implementation of and compliance with this procedure in the following ways;

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 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

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

APPENDIX 1 - SETTING PASSWORDS (GUIDANCE)

1.0 PURPOSE

1.1 The purpose of this guidance is to enable the maintenance of integrity across the Trust's information systems.

1.2 In line with the ITT Security Procedure it is essential that all Trust staff are aware of their responsibilities to maintain the accuracy, availability and integrity of information held in Trust computer systems.

1.3 The document describes the rules about password maintenance, the standards for the management of access controls in computer based information systems.

2.0 COMPUTER PROTECTION

2.1 Password protection has been used for several years to control access to mainframe computer systems. More recently, passwords have also been implemented in the personal computer and Local Area Network (LAN) environments.

2.2 **What is a password? -** Your computer is your personal key to a computer system. Passwords help to ensure that only authorised individual's access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share a password with a colleague or a friend, you may be giving an unauthorised individual access to the system. What if the individual gives your password to someone else? What if some of your files are deleted or otherwise rendered unusable? Are you willing to take the blame if an unauthorised individual uses your access privileges to damage the information on the system or to make unauthorised changes to data?

2.3 Authentication of individuals as valid users, via the input of a valid password is required to access any shared automated information system. Each user is accountable for the selection, confidentiality and changing of passwords required for authentication purposes. Since you are responsible for picking your own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardise the information that they are supposed to protect. Good ones do not.

2.4 Following are some simple rules you should keep in mind about passwords.

- Any system capable of using passwords must have the facility enabled.
- Passwords should be changed frequently. The shorter the life of a password, the better it is. Some systems force users to change their passwords at predetermined intervals.

- Frequency of password change is system dependent and passwords MUST be changed at the frequency appropriate to the system. The default is 30 days for system administrators.
- Passwords should be at least six characters in length. Longer passwords are harder for others to guess.
- Passwords should not be relayed verbally, written down or otherwise revealed to any other individual, either within or outside the Trust.
- Passwords are encrypted (coded) when applied, and therefore cannot be seen by system administrators.
- Never use the same password twice. In fact, good access control systems prevent you from choosing a new password that is the same as your old one. When you are selecting a new password, choose one that is quite different from your previous password.
- Passwords should contain a combination of alphabetic, numeric and special characters (where allowed).
- Avoid using any dictionary words.
- Passwords should not be trivial, predictable or obvious:
    - ***Obvious*** passwords include names of people, pets, relatives, cities, streets, your logon ID, your birth date, car licence plate, and so on.
    - ***Predictable*** passwords include days of the week, months, or a new password that is only one or two characters different from the previous one.
    - ***Trivial*** passwords include common words like ‘secret’, ‘passwords’, ‘computer’, etc.
- Your password should not be the same as your User/Logon ID, an anagram of your User/Logon ID or a palindrome of your User/Login ID. If you have access to a system that require the entry of a password, such as a mainframe computer and a Local Area Network (LAN), try not to use the same password for both systems.
- A good password is relatively easy to remember but hard for somebody else to guess. There are a variety of techniques you can use to choose secure passwords

2.5 The following are examples of these techniques.

1. Use a word with one or two digits embedded in it.
   Examples:

   HOU32SE, MON42DAY, TAB87LE2

2. Make up an acronym based on a nursery rhyme, a favourite song or movie, or a sentence.
   Examples:

   MHALL - **M**ary **H**ad **A** **L**ittle **L**amb; **MDHF#** - **M**y **D**og **H**as **F**leas#; OTGDY - **O**nly **T**he **G**ood **D**ie **Y**oung; **TERM2** - **Term**inator **2**

3. Use a three character pronounceable word suffixed or prefixed with a one- or two-digit suffix or prefix.
   Examples:

   DAM56, WAR34, 56DIG

4. Make up nonsense words that mean something to you by combining the first syllables of two words. However, avoid using standard abbreviations like 'Jan, Feb, Mar, etc.' as part of your password.
   Example:

   PUBPOL - Published **Pol**icy

5. Drop vowels or drop everything but the first 6 letters of a long word or two words.
   Examples:

   CLNDSK1 - **Cl**ea**n D**e**sk, DEDICA5** – **Dedica**tion, **HOMEWO#** - **Home Wo**rk

6. Misspell a word or drop a couple of letters or add some.
   Examples:

   MISTIFI@ - mystify, **CELLEB** – celebrate, **RNYDY$** - rainy day

7. Be creative! And, try to choose a pattern that has meaning for you but that no one else can guess. For example, you might use upcoming events in your life. If you, or one of your children has a major essay to write next month, you might create a password reflecting that event.
   Example:

   MAJESS - Major Essay

8. Or if your 4th cousin, twice removed, is coming for a visit you might create a password such as the following one.
   Example:

   4CUZZ029

9. Another pattern could be to choose meaningful words with a minimum of 10 letters and always use only the first 6 letters. Then add a special character as one of the characters.
   Examples:

   ANNIVE$ - anniversary, **UNBEND#** - unbendable, @**UNBEND** – unbendable, **UN#BEND** – unbendable

10. The best password is one which is a random combination of numeric and alphabetic characters.
    Example:

    48KK439V

***NOTE*: Do not use any of the password examples shown in this document**

11. Finally, please remember that there is no need to share ID's and Passwords. Anyone who needs and qualifies for access to a computer system should submit a request for his / her own Logon ID and password.

2.6 Access to corporate systems will only be given once adequate training has been received and competency levels have been reached, as determined by the trainer / system manager.

3.0 FILE PROTECTION

3.1 Password protection should also be used to protect individual files / documents being transferred across e-mail systems, particularly when passing over person identifiable / sensitive data to external systems / organisations.

3.2 File / document passwords should be applied to all internal transfers of information where it includes person identifiable / sensitive data, as a good practice measure.

3.3 In addition, where regular transfer of such data is required, setting up of shared drives for identified users (i.e. circulation lists for minutes) and giving only appropriately authorised people access would be good / best practice.

4.0 ADDITIONAL GUIDANCE

Refer also to CP9 /CPG9 Records Management Policy / Procedures.
Refer also to CP50/CPG50 Information Governance and Security Policy / Procedures

Essex Partnership University
NHS Foundation Trust

IT&T SECURITY PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG50a
VERSION NUMBER:	3.0
KEY CHANGES FROM PREVIOUS VERSION	Three year review Amendment to Summary and Monitoring Statement s7.8.1 amended s4.2 rescinded
AUTHOR:	Cyber Security Manager
IMPLEMENTATION DATE:	November 2020
AMENDMENT DATE(S):	March 2018; May 2020; July 2020, October 2020; August 2021; May 2022
LAST REVIEW DATE:	May 2022
NEXT REVIEW DATE:	May 2025
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	March 2022
RATIFICATION BY QUALITY COMMITTEE:	May 2022 (Chair's Action)
COPYRIGHT	

PROCEDURE SUMMARY
The procedural guideline supports the Information Governance and Security Policy and will reduce 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). An uncoordinated approach to its safe use 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.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
The Quality Committee will have overall accountability for overseeing the implementation of this procedure within the Trust. The Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this procedures, taking forward any action relating to security as appropriate.

Services	Applicable	Comments
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

IT&T SECURITY PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

IT&T SECURITY PROCEDURE

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 security and apply to all business functions and cover all information systems, networks, physical environment and relevant people who support those business functions.

1.2 Areas of information governance / security covered within the body of these procedural guidelines include:

- Security for Job Definitions & Resourcing
- Security Control of Assets
- Personal Security
- Physical / Environment Security
- Communications
- Access Control
- Systems Development
- Business Continuity

2.0 SECURITY FOR JOB DEFINITIONS AND RESOURCING

2.1 The objective of Security for Job Definitions and Resourcing is to reduce the risks of human error, theft, fraud or misuse of facilities. To ensure that users are aware of information security threats and concerns, and are equipped to support the Trust's security policy in the course of their normal working practices.

2.2 Job definitions

2.2.1 Security should be addressed at the recruitment stage and be included in staff job descriptions and contracts, and monitored during employment.

2.2.2 Managers should ensure that where staff are required to use IT&T they are briefed and encouraged to have sight of the Information Governance and Security Policy CP50) and associated legislation including the Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR), Freedom of Information Act 2000, Copyright, Designs and Patents Act 1988 and Computer Misuse Act 1990 etc. Staff should also be made aware of conduct and disciplinary procedures, which may be invoked should a breach of security arise.

2.2.3 **All** staff are accountable for the functions they perform.

2.2.4 It is essential that significant work performed by any key staff can be taken over by someone else in the event of the unavailability of the key person.

2.2.5 Expertise should be shared. For critical systems, training should be given to at least two staff so that in the absence of one, work may continue in the critical area by the other.

2.2.6 Staff should be fully aware of the extent of their authority, particularly their individual tasks and budgetary responsibilities.

2.2.7 IT&T privileges and access rights should be allocated on the basis of the specific job function, and not on the status or standing of the job.

2.2.8 Personal interest should be declared in circumstances that could lead to a conflict of interest. This is of specific importance where IT&T procurements are involved.

2.2.9 Contractors should be notified of the IT&T security procedures and should sign an agreement to which they must abide. These are the same codes of conduct and discipline as permanent staff. Where contractors are employed through an agency the conditions should form part of the contract with the agency. If work of a sensitive nature is to be performed by contract personnel then extra conditions should be identified and imposed in accordance with this greater risk exposure.

2.2.10 Reference requests during recruitment should also indicate IT&T security matters.

2.3 Confidentiality Agreement

2.3.1 Users of IT&T equipment will sign a non-disclosure undertaking (confidentiality agreement). This understanding will form part of the contract of employment and the conditions in the undertaking should be clearly explained.

2.3.2 Where agency and contract staff and other third party users are not already covered by a non-disclosure undertaking in their existing contract they must sign a confidentiality agreement before they are connected to the Trust's IT&T facilities.

2.3.3 Confidentiality agreements should be the subject of review where there are changes to terms and conditions for employed staff or for contractors.

2.3.4 Where employees or contractors leave:

- The manager should confirm that the confidentiality agreement will continue to apply even though the person is leaving;
- Passwords and combination security doors should be changed to deny access, either by design or accident;
- Relevant departments should be informed of the changes;
- The name should be removed from all Trust directories, including email;
- All Trust property must be returned, particularly personal identification, entry keys, computer equipment and mobile devices;
- Emails cleared in the event of an NHSmail account (as address taken with the employee)

2.3.5 Particular attention should be paid to the above if the employment termination is not 'amicable'.

3.0 DEFINITIONS

3.1 ***IT&T*** – Information Technology & Telecommunications

3.2 ***The Trust*** – Essex Partnership University NHS foundation Trust (EPUT)

3.3 ***Network Assets*** – A collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by various means and created to share data, software, and peripherals such as printers, modems, fax machines, internet connections, CD-ROM and back-up tapes, hard disks and other data storage equipment.

3.4 ***Information Assets*** – (examples below)

<table>
<tr><th>Personal/Other Information</th><th>Software</th></tr>
<tr><td>Databases and data files, Back-up and archive data, Audit data, Paper records and reports,</td><td>Applications and System Software, Data encryption utilities, Development and Maintenance tools,</td></tr>
<tr><th>System/Process Documentation</th><th>Hardware</th></tr>
<tr><td rowspan="2">System information and Documentation, Operations and support procedures, Manuals and training materials, Contracts and agreements, Business continuity plans,</td><td>Computing hardware including PCs, Laptops, PDA, communications Devices e.g. blackberry and removable Media,</td></tr>
<tr><td>Miscellaneous</td></tr>
<tr><td></td><td>Environmental services e.g. power and air-conditioning,
People skills and experience.</td></tr>
</table>

3.5 ***Removable Media*** – Includes back-up tapes, external & removable hard drives, DVD, CD-ROM and Memory Sticks (encrypted USB storage devices).

3.6 ***Confidential Sensitive / Person-Identifiable Information (PII)*** – Includes; person's name, address, full postcode, and date of birth; pictures, photos, videos, audio tapes or other images of patients/residents; NHS number and local identifier codes and anything that could be used to identify a patient or resident directly or indirectly e.g. rare diseases, drug treatments or statistical analyses which have very small numbers in a small population.

*** *Please note*** that the list above is not exhaustive.

3.7 ***Faults*** – Examples below (All faults need to be reported to the IT Service Provider helpdesk via email/phone);

- Computer not switching on
- Encryption / Passwords need to be changed or reset
- Printer not working
- Network drives have disappeared

*** *Please note*** that the list above is not exhaustive.

4.0 SECURITY CONTROL OF ASSETS

4.1 All major Trust assets should be accounted for and have a nominated owner for security purposes. Owners will have responsibility for maintaining appropriate security measures. Responsibility for implementing relevant security measures may be delegated, although accountability should remain with the nominated owner.

4.2 Information security classifications will be used to indicate the level and priority of security protection, including:

"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;

"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.

Confidentiality (NHS Code of Practice)

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.

- It is a legal obligation that is derived from case law.
- It is a requirement established within professional codes of conduct; and It must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

5.0 PERSONNEL SECURITY

5.1 **Personnel security** must be addressed at the recruitment stage and should serve the purpose of:

- Providing direction to the Trust on personnel security and ensure that appropriate personnel security structures are in place regarding awareness training to new Trust employees concerning their information security responsibilities.
- Ensure that procedures are in place to reduce the risks of human error, theft, fraud or misuse of Trust facilities, and to ensure that all staff are aware of the requirement to maintain the confidentiality of information and the security of information processing facilities.

5.2 **Including Security in Job Responsibilities**

5.2.1 Every job description must outline the following points:

- An employee's responsibilities regarding information security.
- That employees are required to be aware of the Trust's policy on information security.
- That employees are responsible for security in relation to their job role.
- Employees should be familiar with other related trust policies, including Information Classification, Data Protection and Confidentiality Policy and security incident reporting procedures.

5.2.2 Contracts must clearly state that any breach of, or refusal to comply, with Trust policies is a disciplinary offence, which may lead to disciplinary action.

5.3 **Personnel Screening Management of staff access to sensitive information**

5.3.1 The Trust will ensure that verification checks are undertaken on all new employees, whether permanent, temporary or contractors, in line with current recruitment policies.

5.3.2 Where staff are employed by other organisations (e.g., agencies), the supplying organisation's contract must set out the responsibilities to undertake relevant checks to a similar level on all staff who will work within the Trust.

5.3.3 The performance of all staff in respect of information security, especially those who have access to sensitive information, should be reviewed on a regular basis by line management.

5.4 Confidentiality Agreements

5.4.1 All employee contracts will include a confidentiality and non-disclosure clause, and must also include reference to the employee's legal responsibilities under the Data Protection Act 2018, General Data Protection Regulation and Computer Misuse Act 1990.

5.4.2 Individuals who are not employed or contracted to the Trust but who have access to, or may come into contact with, confidential information must sign an appropriate confidentiality agreement before access is permitted (e.g. work experience staff who may have access to confidential information).

5.5 Terms and Conditions of Employment

5.5.1 The employee's terms and conditions of employment will clearly state what their responsibilities are regarding security and confidentiality of information within the Trust.

5.6 Information Security Education and Training

5.6.1 The Trust will ensure that all employees are provided with appropriate training in information security as part of their induction process, and are provided with an additional mandatory training programme to update their information security awareness on an annual basis.

5.6.2 The Trust will also ensure that all employees are made aware of updates to the information security policies, and that these policies are readily available.

5.7 Responding to and Reporting Security Incidents, Weaknesses and Malfunctions

5.7.1 The Trust will ensure that all employees are made aware of the information security incident reporting procedures (CPG50(E)) and that they understand the requirement and process for reporting such incidents.

5.7.2 All Trust employees are responsible for reporting information security related incidents, weaknesses and malfunctions as soon as practicable after they are discovered.

5.7.3 All information security related incidents must be reported to the Trust's Information Governance Manager (Information Security Officer/s designate), or to the Director of ITT using the procedure identified in CPG9(F) (Records Management Policy – Information Security Incident Management Procedure).

5.8 Learning from Incidents

5.8.1 The Director of ITT must ensure that all reported information security incidents are recorded in the Information Security Register to ensure that monitoring costs and impacts of all incidents can be carried out across the Trust. All information security related incidents will be reported to and reviewed by the Information Governance Steering Sub-Committee.

5.9 Disciplinary Process

5.9.1 Any violation of these security procedural guidelines or related policies will be handled in accordance with the Trust's Disciplinary Policy and Procedures.

6.0 PHYSICAL / ENVIRONMENTAL SECURITY

6.1 Physical Security / Securing Offices, Rooms and Facilities

6.1.1 Access to data held on the Trust's information systems can be minimised by restricting physical access to Trust buildings.

6.1.2 Signage for buildings, offices and other areas should only give the minimum indication of purpose.

6.1.3 Where information is kept in offices, access to buildings must be restricted. These restrictions include making sure security doors are closed properly and entry codes are changed regularly (see also RM09 Management of Security Policy).

6.1.4 Within any area there should be the facility to protect information and information processing facilities. These facilities may be lockable offices or filing cabinets. As far as possible staff should use these facilities to safeguard and protect information.

6.1.5 Doors and windows should be locked when unattended, with external protection considered for windows, particularly at ground level.

6.1.6 Visitors to non-patient/non-resident areas in Trust buildings should be accompanied at all times and should sign in and out of premises on arrival and departure.

6.2 Equipment Security

6.2.1 In order to prevent loss, damage or compromise of assets and interruption to any Trust business activities all equipment should be physically protected from security threats and environmental hazards.

6.2.2 Protection of IT&T equipment is necessary to reduce the risk of unauthorised access to information and to safeguard against loss or damage.

6.3 Equipment Siting and Protection

6.3.1 For areas where corporate servers are stored the appropriate environment should be maintained (e.g. temperature, humidity and power supply quality).

6.3.2 Corrective action will be taken when any of the above is detected, normally on behalf of the Trust by IT&T staff, using maintenance support arrangements

6.3.3 The Trust operates a no smoking policy in all buildings and locations and eating and drinking are not allowed in designated computer rooms.

6.4 Power Supplies

6.4.1 It is the policy of the Trust to protect critical equipment (e.g. clinical and corporate systems) from power failure. A suitable supply, as dictated by manufactures' specification, will be available, with backup power supplies available when required.

6.5 Equipment Maintenance

6.5.1 Ongoing maintenance of computer equipment will normally be subject to a maintenance agreement. However, under certain circumstances it may be more cost effective to replace equipment rather than continue to maintain. Under these circumstances the Director of ITT will decide whether this course of action will be beneficial to the Trust.

6.5.2 System engineers allowed into Trust premises must identify themselves as belonging to the maintenance company, and must adhere to the general procedures adopted for all visitors.

6.5.3 Where an information medium (e.g. computer hard drive, tape) has failed, the rectification process must result in the failed item being left with the Trust for secure destruction.

6.6 Security of Equipment off Premises

6.6.1 Equipment taken off Trust premises should only be done with the approval of the appropriate manager or Head of ITT Service Delivery. Laptop computers will be protected by suitable access protection and drive encryption. Staff who have obtained authorisation to take equipment off of Trust premises should ensure that such equipment is given a high level of protection. Equipment must not be left in cars as the high incidence of car theft leads to a substantial level of risk for the Trust's equipment and information.

6.7 Secure Disposal of Equipment

6.7.1 All items of equipment that store data must be disposed using the Trust's ICT service provider.

6.8 General Controls – Clear Desk/Clear Screen Policy

6.8.1 Information left unattended on desks or displayed on computer screens is liable to unauthorised disclosure, modification or removal. The Trust operates a 'clear desk' and 'clear screen' policy, covering paper information, removable storage media and information displayed on computer screens. Where appropriate, paper and computer media containing sensitive information should be stored in suitable locked cabinets when not in use. Computers / telephones must not be left logged on when unattended.

6.8.2 Sensitive or confidential information, when printed, must be removed from printers, photocopiers and fax machines immediately. Incoming and outgoing mail points and fax machines must be protected from unauthorised access. Where information is transferred by fax, appropriate measures must be

taken to ensure that there is no accidental disclosure. Reference should be made to Trust policy CPG9(E) Safe Haven Procedure.

7.0 COMMUNICATIONS & OPERATIONS MANAGEMENT

7.1 This section provides guidance in the following areas:

- The secure operation of information processing facilities
- The minimisation of risk of system failures
- The protection and maintenance of the integrity and availability of software, information and information processing and communication facilities.

In addition:

- To ensure that information within networks and their supporting services is adequately protected
- To ensure the Trust assets are protected and that interruption to business activities is minimised.
- To prevent loss, modification or misuse of information.

7.2 Operational Procedures and Responsibilities

7.2.1 The Trust must ensure that all operating procedures identified within the IT&T Security procedure are documented and maintained. Changes to these documents must be authorised by Director of ITT. Operating procedures must specify the detailed instructions for the implementation of each job, including:

- Processing and handling information, including confidentiality requirements and information classifications.
- Work scheduling requirements.
- Instructions for handling errors or other exceptional conditions, including restricting the use of system utilities.
- Contacts for support in the event of technical or operational difficulties.
- Any instruction for handling special stationery or other special system outputs.
- Detailed system start and recovery procedures to be followed in the event of a system failure.
- Procedures for system housekeeping, backups, equipment maintenance, and computer room usage.

7.2.2 Changes to information processing facilities and systems must be controlled. The Trust must have in place formal documentation change control mechanisms, including:

- Identification and recording of significant changes and assessment of their potential impact.
- Formal approval for proposed changes.
- Communication of changes to all relevant personnel.
- Procedures for aborting and recovering from planned unsuccessful changes.

7.2.3 The Trust must have in place documented Incident Management Procedures to ensure an effective response to information security incidents.

7.2.4 The Trust should, where appropriate, ensure that segregation of duties is in place on all systems, in order to reduce the opportunities for unauthorised modification, or misuse of information and information systems.

The Trust must also ensure that, where possible, development, test and operational facilities are segregated. Where possible, development and operational systems should be run on different processors, or in different domains or directories.

7.2.5 Where an external contractor is used to manage processing facilities, the Trust must ensure that an appropriate risk assessment has been undertaken and that appropriate controls have been agreed to reduce any potential exposure to damage or loss of information. These controls must be incorporated into any contracts that are established.

7.3 System Planning and Acceptance

7.3.1 The Trust must ensure demands on system capacity are monitored and projections of future capacity requirements are made to ensure that it has adequate processing and storage facilities available. The utilisation of key system resources, such as file servers, e-mail servers and business critical systems should be monitored so that additional capacity can be brought online when required.

7.3.2 The Trust must have in place acceptance criteria for new information systems, for upgrades and new versions. All such changes must be tested prior to acceptance.

7.3.3 Specific responsibility for planning network facilities and change control of the network rests with the Director of ITT. The IT&T Department shall maintain a comprehensive plan of the network, documenting all major components and cable structures.

7.3.4 Any new cabling installations shall be planned to reduce the risk of unauthorised physical tampering or connection. All cabling running 'public access' areas should be hidden in roof spaces or ducting to minimise the risk from malicious damage.

7.3.5 A standard, documented directory structure shall be implemented across all network file servers. All users shall be provided with a directory for the storage of business files. All other directory allocations shall be documented and based upon specific business needs.

7.4 Protection against Malicious Software

7.4.1 The Trust must have in place formal controls to detect and prevent malicious software from entering the network. These controls must, as a minimum, include:

- Compliance with software licensing.
- Compliance covering obtaining and introduction of files and software either from or via external networks.
- Installation and regular update of anti-virus detection and repair software.
- Procedures for dealing with viruses and business continuity plans for recovering from virus attacks.

7.5 Housekeeping

7.5.1 In order to allow the Trust to recover as quickly as possible in the event of data loss or corruption on one or more of its computers systems data essential to the business of the Trust must be backed-up. In order to achieve this there must be set procedures to cover:

- The copying of data to a medium, which can then be stored in a secure location (back-up).
- The retrieval of data from copy made on the selected medium (restore).
- The secure storage of media containing the data containing the data copies.
- The recording of details about the media and what data is stored in order to facilitate the easy and correct identification of a particular item of storage media when it is necessary to retrieve data from it.
- Testing the quality of the back-ups made both by log checking, verification and by test retrieval of data from an item of storage media.

7.5.2 The Trust must ensure that all faults reported by users regarding problems with information processing or communications systems are logged, along with the corrective action taken.

7.6 Network Management

7.6.1 The Trust must ensure that appropriate mechanisms are in place to all protect Trust Networks from unauthorised access and to protect the security of data within the network and connected services. Where possible the following should be adopted, including:

- Operational responsibility for the network should be separated from computer operations, where appropriate.
- Responsibilities for the management of remote equipment and remote access to the network must be identified.
- Where appropriate, special controls should be implemented to protect the integrity of information passing over public networks, such as the use of encryption and digital signatures.
- The network architecture should be specially documented, including the planned detailed settings of all hardware and software components.

7.7 Media Handling and Security

7.7.1 The Trust must put in place procedures for the appropriate handling and security of removable computer media such as tapes, disks, memory sticks / flash drives (USB devices), cassettes and printed media (reports). Procedures should include the requirement to erase the previous contents of any re-usable media when no longer required, formal authorisation for the removal of media from the Trust and the requirement for media to be stored in a secure manner

7.7.2 The ICT service provider is responsible for the secure destruction of all data media that is no longer required

7.7.3 The handling and storage of information must be conducted in line with the GDPR & Data Protection Act 2018

7.8 Information and Software Exchange

7.8.1 In order to prevent loss, modification or misuse of information the Trust should ensure that the exchange of information and software between organisations should be controlled by the adherence to the HSCN (Health and Social Care Network), and any agreed Data Sharing Protocols.

7.8.2 The exchange of information and software between organisations should be controlled. For physical transport, reliable couriers should be used at all times. Where necessary, special measures should be adopted to protect sensitive information from unauthorised disclosure.

7.9 Security of Electronic mail

7.9.1 When using the electronic 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.

7.9.2 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 (i.e. NHSmail (@nhs.net) for the secure transfer of person identifiable information via email).

7.10 Permitted use

7.10.1 Trust staff should use email for business purposes, including sending patient/ resident data (following assessment of risk and application of controls, such as password protecting documents).

7.10.2 IT&T services uses software to monitor the use of emails and can intercept inappropriate attachments, which will be reported to the Trust's Data Protection Officer/s as a breach of the GDPR & Data Protection Act 2018.

7.10.3 The Trust authorises Limited 'personal use' of its email facilities.

7.11 **Non-permitted use**

7.11.1 Staff must not use the Trust's email facilities for excessive personal use, or private gain. Sending offensive, defamatory material or breach confidentiality is also forbidden. Any such breaches may be subject to the Trust's disciplinary procedures.

7.12 **Security of Electronic Office Systems**

7.12.1 The Trust's electronic information resources are vital assets, which require appropriate safeguards. Electronic office systems are vulnerable to a variety of threats, which may compromise the confidentiality, integrity and availability of information.

7.12.2 Electronic office systems includes Calendar, systems such as Outlook, Word processing, spreadsheets, databases and underlying electronic infrastructure required to operate such systems. The following controls should therefore be applied:

- All users, along with line managers, are responsible for controlling access to their calendars. Any delegated access should be provided strictly on a 'need-to-know' basis.
- The Trust will provide the infrastructure to allow staff to save files and documents to shared network drives that are regularly backed up.
- Line managers will be responsible for authorising which staff are allowed to access appropriate areas of shared network drives and folders.
- Users are responsible for deleting files when no longer required.

7.13 **Publicly available systems**

7.13.1 Access for Trust staff to certain websites on the internet will be controlled by a request and authorisation process, and monitored by IT&T.

7.14 **Information transmitted via telephone, fax and post**

The following minimum standards will be applied:

7.14.1 Telephone conversations (including answer-phones):

- No personal information shall be given out over the telephone without best endeavours by the member of staff to confirm the identity of the other party, and the wishes of the individual concerned.
- Telephone calls that may feature personal or sensitive information about any individual will be made in private areas if at all possible.
- If an answer-phone message is left, minimal information will be provided.

7.14.2 Fax:

Reference should be made to the Trust's Safe Haven Procedure CPG9(E). However, the following points should be adhered to, including:

- Faxes must be sent to named individuals.
- All Faxes must be preceded by a cover sheet.
- Fax machines must be sited away from public areas.
- Minimal information will be transmitted.
- The intended recipient must be notified prior to sending.
- The Trust must designate specific fax machine locations as a 'safe haven', where patient/resident and sensitive information can be transmitted and received in a secure environment.

7.14.3 Post:

- All post should be sent to a named individual, where possible.
- All post will be marked 'Private and confidential' if it contains personal and/or sensitive information and will not be sent in re-seal envelopes.
- A P.O Box return address should be on the reverse of the envelope.
- Window envelopes should be used – a handwritten address is not advised.

7.15 **Information Transmitted via email and Internet**

7.15.1 All staff should be aware of the procedures relating to email and internet use and should read the Email / Internet Access and Use Procedure (CPG50(B)) for further information.

7.16 **Video Consultations / Video Conferencing (VC)**

7.16.1 Video conferencing is a live audio and video conversation between two or more people in different locations, conducted using phone, tablet, laptop or desktop computer.

7.16.2 The Trust has approved the use of the following applications:

- Microsoft Teams
- AccuRx
- Attend Anywhere

7.16.3 Key considerations regarding the use of VC applications are below:

Users of are reminded of their obligation to complete the mandatory Information Governance e-learning module on an annual basis.

- VC should be used for business purposes in line with Trust Information & Security policies / Record Management policies / professional codes of practice / Data Protection Act 2018 / General Data Protection Regulation 2016.

- Users are reminded that ALL information created within Teams is saved to a library, which is a **temporary** SharePoint site. Teams is designed as a tool to help collaboration, not as a permanent way to store records. Users **MUST** adhere to their professional codes of practice, the policies listed above and contractual requirements to information and records are appropriately managed. Do not use Teams as a permanent records store.
- Teams is not a clinical or workforce system. The disclosure and storage of personal and confidential information should be kept to a minimum and appropriate security measures applied.
- Regularly review Team membership and take account of movers and leavers.
- Consider the information shared during group calls/meetings, especially where participants are external to EPUT. Be aware that participants in group calls may be able to download any shared content and consider whether it is appropriate to share your screen.
- When offering a video consultation, ensure that the method you use to send the invitation is appropriate for the attendee to have, i.e. email address or mobile number. If it is not appropriate for the attendee to know your email address or mobile number, use a generic email account with a disclaimer (out of office response and/or signature) stating that email replies are not monitored.
- Information posted in the chat function of MS teams can be retained by any participant, ensure that any messages or content posted in the chat is appropriate to be shared with all attendees.

You must:

- notify your manager immediately if you receive any inappropriate material.
- comply with copyright law and all applicable licenses, which may apply to software, files, graphics, documents, messages and other material you wish to upload / to download or copy.

You must not:

- access, store or provide links to inappropriate non-business-related websites or other resources which display, store, make available or send material which is illegal, discriminatory, harassing, obscene, pornographic, libelous, defamatory, breaches any obligations of confidentiality or is otherwise deemed by EPUT to be inappropriate in the work place.
- Illegally copy material protected under copyright law or make material available to others for copying.

7.16.3 Recording within MS Teams

Recording meetings can be a useful way of capturing training sessions, allowing colleagues who could not join a meeting to catch up later, or as a reference for note taking afterwards. However, there are a few things that users should be aware of to ensure that the recording is secure, but accessible to the right people.

7.16.4 Five key things to know about recording meetings

1. When you record a Teams meeting it is stored temporarily (for 20 days) in the meeting chat history. Whoever initiates the recording is responsible for it throughout its lifecycle.
2. The recording is available to download by NHS.net staff participants only. Guests are not able to download.
3. Recordings are NOT uploaded to Microsoft Stream and can only be accessed once they are downloaded and saved on a secure network drive".
4. All recordings are subject to professional conduct and Information Governance standards. Please be mindful of what you discuss, record and share.
5. Recordings not downloaded will automatically expire and delete after 20 days and will not be available for download.

7.16.5 Whoever initiates a recording is the owner of that recording, and it is their responsibility to ensure that:

- Everyone being recorded is aware of and in agreement with the meeting being recorded.
- If the recording is downloaded, it is held securely and deleted as soon as it has been used for its specific purpose – for example, if used as a reference to take minutes, the recording should be deleted as soon as the minutes have been approved.

7.16.6 Governance of recordings

Be aware that anything you record could be made available under:

- Freedom of Information (Scotland) Act
- Subject Access Requests, under the General Data Protection Regulations
- Data Protection Act (2018)
- Other authorised and agreed international standards and regulations.

Therefore, be mindful of what is discussed, recorded and shared. If in doubt ask EPUT's Data Protection Officer, Information Governance representative and records managers for advice about data protection and information management.

7.17 **USB 'Memory Sticks'**

7.17.1 A USB device, 'memory sticks', is a mobile storage device, which holds a vast amount of data and can be easily plugged into a notebook or PC USB ports. It is convenient and easy to use, and the user can define a password for confidential data areas. Other names for USB 'memory sticks' include flash drive, pen drive and thumb drive.

7.17.2 **Only encrypted USB 'memory sticks' provided or sanctioned by the Trust** may be connected to any device on the Trust network.

7.17.3 Only IT&T Services will be permitted to purchase USB 'memory sticks', and a Register will be maintained for monitoring purposes.

7.17.4 The USB 'memory stick' must only be used for legitimate work purposes.

7.17.5 Any data held on USB 'memory sticks' must be password protected to protect contents from unauthorised access.

7.17.6 It will be the responsibility of the user to use due diligence to keep memory sticks secure at all times.

7.17.7 No patient or resident identifiable information is to be held on USB 'memory sticks'. They should only be used for transferring the data, then the data should be deleted. This applies only to Trust encrypted USB sticks.

7.17.8 Any loss of USB 'memory sticks' must be reported to the Trust's Data Protection Officer/s or Head of ITT Service Delivery immediately.

7.18 **Other 'Plug-in' Devices**

7.18.1 These devices include, but are not limited to:

- MP3 Players (which can hold more information than USB 'memory sticks')
- Smart Phones (mobile phones, which allow connection to PC's and run
- Various operating systems such as Windows CE
- Digital Cameras
- Compact Flash Cards
- External USB hard drives
- Firewall devices

7.18.2 These 'plug-in' devices are governed by the same 'acceptable use' criteria as with the above-mentioned USB 'memory sticks'

7.19 **Mobile Phones**

7.19.1 Only ITT Services will be permitted to purchase mobile phones and a register will be maintained for monitoring purposes. All mobile phones will be issued encrypted and with password protection and staff are responsible for ensuring they update passwords to a personal setting and then maintain the security of their passwords. It will be the responsibility of the user to use due diligence to keep mobile phones secure at all times.

7.19.2 Only mobile phones provided or sanctioned by the Trust may be connected to the Trust WiFi.

7.19.3 Mobile phones must be returned to ITT services when their intended use by the recipient is no longer needed.

7.19.4 The use of mobile phones for personal use is permitted at cost, however, no support is offered and any data loss resulting from work usage or incident resolution is not the responsibility of the Trust. If the device becomes non-functional through personal usage, the default response will be to perform a factory reset.

7.19.5 Mobile phones will be monitored for activity and usage relating to voice and data. Any excessive use will be investigated and could result in disciplinary action being taken against the member of staff.

7.19.6 If a mobile sim is present in a device, this must at no point be changed or tampered with.

7.19.7 Users should create, maintain and manage an iTunes account for use with the device. Any issues experienced with your account cannot be resolved by ITT services and you will be required to liaise directly with Apple on any such issues.

7.19.8 Dictation can be enabled for users on mobile phones on request via ITT services. It is the user's responsibility to ensure that any configuration changes are followed and maintained to ensure no data is sent to third parties.

7.20 **Laptops or Tablets**

7.20.1 Only laptops provided or sanctioned by the Trust may be connected to any device on the Trust network and these must be used for legitimate work purposes.

7.20.2 Only IT&T Services will be permitted to purchase laptops or tablets and a register will be maintained for monitoring purposes. All laptops or tablets will be issued encrypted and with password protection and staff are responsible for ensuring they update passwords to a personal setting and then maintain the security of their passwords. It will be the responsibility of the user to use due diligence to keep laptops or tablets secure at all times.

7.20.3 No corporately sensitive / patient / resident / staff or other person identifiable information is to be held on laptops or tablets. When using laptops or tablets to work with person identifiable information this can only be done if the staff member has access to the Trust network via VPN (Virtual Private Network) or Work Smart set-ups.

7.20.4 No data should be held on the laptop or tablet's hard drive (C:\) at any time. If using a Trust laptop or tablet device for non-person identifiable data you should not save this to the hard drive but securely e-mail work on to a Trust network as soon as possible. Where a laptop or tablet is connected to the Trust's network information should be saved direct to the network drives.

7.21 **Reporting Incidents**

7.21.1 In the event of failure of any PC (desktop) or portable media device encryption, password or virus protection staff should immediately contact the IT&T service desk for advice and guidance as to continued use or repair requirements.

8.0 ACCESS CONTROL

8.1 Access to information should be controlled on the basis of business and security requirements and the user's role in the operation of the Trust.

8.2 Trust systems need to be strictly controlled to ensure that only those authorised can gain access and that access is defined on the basis of need. Access control is a requirement of current UK legislation.

8.2.1 Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate that processing is performed in accordance with this Regulation**. Those measures shall be reviewed and updated where necessary.

8.2.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

8.3 **System access control**

8.3.1 The following rules will be applied to controlling access to any information system within the Trust by any employee and third parties.

8.3.2 Access to systems and information will be on a 'need-to-know' basis.

8.3.3 Setup and regular maintenance of access controls in systems will take account of all relevant legislation and regulations. Advice should be sought from IT&T, who will in turn seek more specialist advice if required.

8.3.4 Access controls will be based on user roles, clinical speciality and geographical location.

8.3.5 All access controls will be reviewed regularly by IT&T.

8.3.6 As a general rule, certain administration staff should see little or no clinical information, accepting there are some administrative roles that will require access to such clinical information.

8.4 User access management

8.4.1 To prevent unauthorised access to information systems, formal procedures are in place to register access to Trust systems. These include:

- The formal completion of an access application form, which is endorsed by the users' immediate line manager and countersigned by the authorised signatory within IT&T.
- The use of unique user ID's to ensure that users can be linked to, and made responsible for, their actions.
- Maintenance of a formal record of all users.
- Immediate removal of access rights of users who have left the Trust, or changed operational role.

8.4.2 The Trust also ensures that the allocation and use of special privileges (i.e. administrator rights - the ability to override system or application controls) is restricted and controlled.

8.4.3 Access to all critical systems within the Trust is controlled by passwords, and the allocation is controlled through a formal management process.

8.4.4 Regular reviews to user access rights are carried out annually.

8.4.5 The Trust's Human Resource Department should ensure that all leavers are notified to IT&T in order prompt removal of redundant user accounts is carried out.

8.5 User Password Management

8.5.1 Most systems within the Trust require a log in name and password for access. All staff are given access rights and privileges to the various systems in accordance with the type of data they require to use. All staff will have a log- in for one or more of the network servers in addition to any other systems they use.

8.5.2 In all cases any passwords given to staff personally are for that individual only. Passwords should not be written down or given to others to use under any circumstances.

8.5.3 Passwords should be a minimum of 6 characters (see Appendix 1 – Setting Passwords Guidance) and should be a combination of letters and numbers and should be changed every 30 days as prompted on-screen.

8.5.4 Do not use familiar names, such as pet names, and if at all possible try not to use proper words. This makes the accidental discovery of a password more difficult.

8.5.5 Passwords must be kept confidential, and changed if users believe they have been compromised.

8.5.6 Some systems will prompt you when a password change is required, other do not. If they do not it is an individual's responsibility to change them.

8.5.7 If you suspect someone else may have detected your password, or you suspect someone else is using it you must change your password immediately and advise your manager.

8.6 **Computer Security**

8.6.1 All staff are responsible for all data they enter onto Trust computers. The very nature of the type of sensitive information staff deal with makes protection of that information of paramount importance.

8.6.2 All staff have a legal responsibility under the GDPR & DPA18 and the Computer Misuse Act to ensure that unauthorised access to data is prohibited and also that data is accurate and kept up-to-date. Such restrictions apply not only to people outside the Trust but may also apply to those in the Trust whose work does not necessitate access to the data. All staff must abide by the rules of the GDPR, Data Protection Act and Computer Misuse Act.

8.6.3 Never leave your computer unattended when it is logged on. Ensure that the lock facility on your computer is in operation.

8.6.4 Always ensure when leaving your place of work to log off and close down your computer correctly.

8.7 **Network and Operating System Access Control**

8.7.1 Access to Trust networks are restricted to authorised users only via a secure log-on process designed to minimise the opportunity for unauthorised access.

8.7.2 User access is restricted to those functions and applications that are required for the performance their duties.

8.7.3 The IT&T team is responsible for the issue of Network log-in accounts and also for email accounts, and the Service Desk is directly responsible for allocating access rights to staff wishing to access their systems.

8.7.4 Unsuccessful log-on attempts are restricted to three, whereby further attempts are blocked and the user must contact IT&T for verification and resetting of password rights.

8.8 **Remote Access**

8.8.1 Remote access is the ability to get access to a computer or network from a remote distance (i.e. home address).

8.8.2 For staff who require access to their email account the Trust will authorise connection via Outlook Web Access (OWA), which is a client/server remote access software solution based on Microsoft's .NET Framework.

8.8.3 For staff requiring access to the Trust network, including web resources, bespoke programs and network data, connection will be available through the Virtual Private Network (VPN) remote access facility. Reference should be made to

Corporate Policy (CP30), Virtual Private Network (VPN) Remote Access to the Trust Data Network.

8.8.4 Staff wishing to utilise these facilities should contact the Head of ITT Service Delivery.

8.9 **Network Shared Drives**

8.9.1 It is the policy of the Trust to keep all data in a secure manner and to only allow authorised access to files to those who require the data as part of their normal duties. Unless there are specific reasons not to do so, all data files should be saved on the network file servers rather than on local PCs.

8.10 **Viruses**

8.10.1 It is the responsibility of all staff to protect the Trust's computer systems from viruses. All files received on any medium from outside the Trust (including those used on home computers) and any received via electronic mail must be checked for viruses before being used.

8.10.2 The Trust systems use sophisticated software to detect viruses. However, if you receive any emails that you are unsure of, or do not recognise the sender, do not open them. If you are unsure inform your manager.

8.11 **Backups**

8.11.1 The IT&T team will ensure all Trust servers and the files contained within are backed up on a daily basis.

8.11.2 It is the responsibility of individual users to back up any systems, which do not hold their data centrally.

8.11.3 All backups must be kept up-to-date and must be checked on a regular basis to ensure that it is possible to recover the data on them.

8.12 **Mobile Computing**

8.12.1 The Trust will ensure that mobile computing facilities are adequately protected to ensure that business information is not compromised. All staff whom use mobile computing facilities will receive adequate training and be aware of the increased security risks associated with storing information on these devices.

9.0 SYSTEM DEVELOPMENT & MAINTENANCE

9.1 To ensure that information governance controls are built into information systems and information processes, governance requirements will be built into systems from the outset. Suitable controls will ensure that management of purchasing new systems, together with the enhancement of existing systems, will ensure that information security is not compromised.

9.2 Security Requirements of Systems

9.2.1 The information governance lead will be involved in the development of new and existing information systems in order to provide advice on the appropriate security requirements, together with best practice for implementation.

9.2.2 IT&T system managers will be responsible for ensuring that appropriate security arrangements have been included in system specifications for new systems and system upgrades, and that all modifications to systems are logged and up-to-date documentation exists.

9.2.3 The I nformation governance, Data Protection Officer and Caldicott leads will ensure that full compliance with the GDPR, Data Protection Act 2018, common law duty of confidentiality and Caldicott requirements are paramount concerns of system and process developments.

9.3 Security in Application Systems

9.3.1 Application systems, wherever possible, will provide validation of all input to ensure that it is correct and appropriate. The following controls should be considered:

- Out-of-range values and invalid characters.
- Missing or incomplete data.
- Periodic review of the content of mandatory fields, or data files, to confirm their validity and inspection of hard copy input documents for any unauthorised changes.
- Defining responsibilities of staff involved in input processes.

9.3.2 Validation checks will be incorporated into systems in order to detect corruption of data that has been correctly inputted.

9.3.3 The new NHS Number should be used as the common identifier on all patient / resident records and correspondence. Local identifiers (e.g. hospital numbers) may be used.

9.3.4 The responsibility for review and development of input / collection validation will lie with the Director of ITT

9.3.5 Line managers of staff will have default responsibility to ensure their staff are aware of processes and procedures relating to the quality of inputted data.

9.3.6 Until such times as no further required, the Trust's Clinical Governance Audit Team will conduct a routine audit of paper-based records.

9.4 Security of System Files

9.4.1 All modifications to systems, including changes, updates and servicing of hardware, as well as software, must be conducted with security of paramount importance.

9.4.2 All software must be quality tested before general use. Where possible IT&T should test the reliability of any new or updated systems by running them in parallel with the old prior to installation.

9.4.3 Supplier software, which is used in systems, must be maintained at a level supported by the supplier, and any decision to upgrade must take into account the security of the release. Physical access should only be provided to suppliers for support purposes when necessary and must be with IT&T senior management approval. All supplier activity on systems must be monitored

9.5 **Security in Development and Support Processes**

9.5.1 Changes to any system must be assessed under a formal change control system. This must include an assessment of any changes and the impact on existing security. A record of all changes made must be logged, and must include:

- The identity of the person making the change
- Details of the changes made
- Any other systems affected by the changes
- Date and time of the change, with test results

9.5.2 When changes to operating systems are performed, application security should be reviewed to ensure that there is no adverse impact on existing security.

9.5.3 Access to data should wherever practical be limited to anonymised data and must be authorised by the data owner. Copies of data must be retained at the same levels of security and access controls as the original data. No testing must take place on 'live' data, including training or demonstration purposes.

10.0 BUSINESS CONTINUITY PLANNING

10.1 Business Continuity planning ensures that the Trust's essential business activities will be maintained in the event of any unforeseen major failure or disaster.

10.2 **Business Continuity Management**

10.2.1 The Trust is increasingly reliant on IT&T services in support of patient/ resident care. Any emergency affecting business critical systems may have a significant impact on the Trust's ability to continue its operations. Procedures must be developed, based on a Risk Assessment to recover affected systems and processes in order to ensure continuing operations within the Trust.

10.3 Business Continuity Process

10.3.1 The Trust will ensure that a managed process is in place for the maintenance of business continuity. The process must include:

- Understanding and identifying the risks to the Trust, this could result in the loss of vital systems or processes in terms of their likelihood and impact.
- Identifying and understanding the impacts, which interruptions are likely to have on the formulating and documenting business continuity plans for each of the Trust's business critical systems and processes.
- Regular testing and review of the plans and processes put in place.
- Ensuring that the business continuity plans are communicated throughout the Trust and that all affected staff are aware of what actions to take in the event of an emergency.
- Ensure that responsibility for the co-ordination of business continuity management is assigned at the appropriate level within the Trust.

10.4 Business Continuity Planning Framework

10.4.1 It is essential that there is a realistic continuity plan for each operational computer system, which identifies its essential elements and details the action to be taken to maintain these in the event of software or equipment failure. In the case of critical/corporate operational systems, continuity plans must be based on the availability of back-up computing facilities. The continuity planning process must include:

- A formal documented assessment of how long users could manage without each computer system.
- A formal documented assessment of the criticality of each system, including the impact on the short, medium and long term loss of the system on business activities.
- Identification and agreement of all responsibilities and emergency arrangements.
- Documentation of agreed procedures and processes.

10.4.2 The Head of ITT Service Delivery will ensure that appropriate continuity plans are drawn up for all relevant systems.

10.4.3 The regular review of systems must also include the checking of continuity plans and that all staff receives relevant training, that documentation is up-to- date and that continuity plans are always is a 'state of readiness'.

10.5 Testing and updating Business Continuity Plans

10.5.1 The Trust must ensure that a testing schedule is in place, which sets out which elements of the plan are to be tested, when they are to be tested and who has responsibility for ensuring that the testing takes place. All tests should be monitored and documented.

10.5.2 Business Continuity Plans must be updated in the following circumstances, including:

- Changes to key personnel.
- Changes to contact details of personnel or system suppliers.
- Changes to location, facilities and resources
- Changes in legislation
- Changes to suppliers
- Changes to system or processes and identification of any new risks.

END

Appendix 1
March 2016

Received _____ Entered _____

Network Change Control Form

New User	[ ]	Relocating within the Trust	[ ]
Changing Personal Details	[ ]	Additional Access	[ ]

Please fill out the details correctly for the return slip to be sent back

Name:
Job Title and Department:
Site:
Telephone number:

Do you use a Cisco Phone:	Yes	No

Please state additional access requirements e.g. shared folder, client information
If you require access to any other system, e.g. WinDip, Cedar, Care Plus please complete
the relevant form for that system which can be obtained via the Intranet

User Signature:

Date: Please Print Name:

Please check the above details

Manager Signature

Date: Please print Name:

Please check the above details

System Owner Signature:

Date: Please Print Name:

Director Signature (**only if Internet access is required**)

Date: Please Print Name:

Cut along line

To be completed by the IT&T department and sent back to user

Username

E-mail address firstname.surname@nhs.net

Please phone the IT&T Service Desk on 01375 364487 to get your password and to setup your e-mail account

Essex Partnership University
NHS Foundation Trust

INTERNET AND INTRANET ACCESS AND USE PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG50b
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	Reference to email removed–covered in CPG50H –NHSMail Usage Procedure (Procedure B to be renamed) Sections 5 –9 rescinded (email focussed) Other references to email deleted throughout
AUTHOR:	Head of IT Infrastructure, Cyber & Assets & Deputy Data Protection Officer
CONSULTATION GROUPS:	DSPT & Risk Working Group, Information Governance Steering Sub-Committee
IMPLEMENTATION DATE:	May 2018
AMENDMENT DATE(S):	February 2019, March 19); Dec 2019 Sept 2020 , Aug 2022; March 2023
LAST REVIEW DATE:	March 2023
NEXT REVIEW DATE:	March 2026
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	October 2022
RATIFICATION BY PORG:	March 2023
COPYRIGHT	

PROCEDURE SUMMARY		
The purpose of this Policy is to provide best practice standards for the enforcement of a Trust wide Internet and Intranet Access and Use Procedure that meets the guidance laid out by NHS Digital and the National Cyber Security Centre.		
The Trust monitors the implementation of and compliance with this procedure in the following ways:		
Continual monitoring by ICT Services		
Services	**Applicable**	**Comments**
Trust wide	✓	

The Director responsible for monitoring and reviewing this procedure is Director of Information Technology and Telecommunication

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INTERNET and INTRANET ACCESS AND USE PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

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 internet and 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 internet and 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 internet and 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 internet and intranet systems. The policy applies to the Trust's employees and others carrying out work on behalf of the Trust.

2.2 The purpose of this procedure is to clearly explain what is acceptable and unacceptable when using the Trusts Internet and 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.
- Ensure that their staff follow this procedure

3.3 ***Employees must:-***

- Make themselves aware of this procedure and follow it whenever they access the internet and intranet.
- Not share the access privileges that they have been granted with others.
- Not use others' access privileges to access the internet or intranet systems.

3.4 ***Deputy Director of IT must:-***

- Ensure the continued management of information technology security.

3.5 ***IT Support Staff must:-***

- Only install and give access to the internet and intranet systems after the request for access has been authorised.
- Record activity by the Trust employees on internet and intranet systems.
- Regularly review the security effectiveness of the means of access.

4.0 DEFINITIONS

4.1 **Patient or Residents /Personal Information**

" ***Personal Data"***
Means any information relating 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

4.2 **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.

4.3 **Chat Rooms**

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

4.4 **I.P. Address**

- This is the unique address for your computer.

5.0 USING INTERNET and INTRANET SYSTEMS

Acceptable Use:-

5.1 The internet and 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.

5.2 Any internet and 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').

5.3 Those that use Trust internet and 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.

5.4 Access to Trust internet and 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.

5.5 Access to internet and 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.

5.6 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).

5.7 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:-

5.8 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.

5.9 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

5.10 Where staff inadvertently access websites which may fall into the group above (9.9) this should be reported to the Trust's ITT Service Desk (via the "Get IT Help" portal) immediately.

5.11 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.

5.12 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:-

5.13 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.*)

6.0 MONITORING INTERNET AND INTRANET SYSTEMS

6.1 A username and password restrict the use of internet and intranet 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.

6.2 Trust staff must not share usernames or passwords with colleagues.

6.3 In the event of abuse/misuse of the Trust's internet and intranet 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.

6.4 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.

6.5 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 and 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.

6.6 If a breach of internet and 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

SAFE HAVEN PROCEDURE – CPG50(C)

Appendix 1

1.0 Safe Haven Incoming and Outgoing Faxes

Fax is only permitted for use in the Trust Pharmacy Service.

2.0 Safe Haven Electronic Information (transfer by Email)

2.1 **Do's for Electronic Information**

2.1.1 Confidential information can be sent between NHSmail accounts – but only when essential to service delivery. Where Line Managers / Directors expressly require information to be transferred via this method the ITT Servicedesk should be contacted, who will arrange for an NHSmail account to be set up. (The email will be encrypted automatically).

2.1.2 Confidential information transferred by email must only be carried out using specifically registered, authorised and secure devices (e.g. encrypted desktop or laptop) and only in accordance with Trust approved policies and procedures. (Personally owned devices must not be used under any circumstances).

2.1.3 Suitably approved back up and fail safe facilities must be in place and operating satisfactorily before confidential information is transferred by email.

2.1.4 Where transfer of person identifiable confidential information by email is allowed; this must be sent as encrypted / password protected attachments (and not in the body of the email) through NHSmail accounts, wherever possible.

2.1.5 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).

2.1.6 Where transfer of confidential information by email is allowed, a secure "mechanism" must be in place to trace all confidential information.

2.1.7 The address of the recipient must first be confirmed, together with a test message also confirmed.

2.1.8 When emails are used to transfer confidential information the email subject should clearly be marked "confidential".

2.1.9 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.

2.1.10 Email transferring confidential information must carry a Trust approved disclaimer for confidential information (see below 4.2.1.1).

2.1.11 The following email domains are secure for sending person identifiable information to external organisations:

Secure email domains in ***central government***: *gsi.gov.uk, *gse.gov.uk, *gsx.gov.uk. The ***Police National Network/Criminal Justice Services*** secure email domains: *.police.uk, *.pnn.police.uk, *.scn.gov.uk, *.cjsm.net. Secure email domains in ***local government / social services***: *.gcsx.gov.uk
However these are subject to change so please check first.

2.1.12 The intended recipient must adhere to the principles of safe haven (i.e. to ensure that confidential information is only viewed by persons authorised to view such information).

2.1.13 Confidential information sent to the Trust by e-mail must be virus checked before it is opened.

2.1.14 Confidential information sent to the Trust by email must only be stored on Trust registered secure network servers. (It must not be stored on PC's, laptops, ipads and other portable devices or removable media).

2.1.15 **Disclaimer: "***This document and any attachments to it are confidential and privileged and intended solely for the use of the individual or entity to whom they are addressed. They should not be disclosed, copied or distributed without the prior authorisation of the author. Use of / action taken in relation to its contents is strictly prohibited and may be unlawful. In the event of mis-direction please notify sender."*

2.2 **Don'ts for Electronic Information**

2.2.1 Confidential information must not be sent by email unless it is encrypted / password protected to NHS approved standards and using software authorised and configured by the Trust.

2.2.2 Staff are not permitted to send confidential information in relation to patients, employees or the public via Internet Mail (e.g. Yahoo, Hotmail etc.).

2.2.3 Confidential information must not be sent in the open body of the email. An encrypted / password protected attachment must be used or sent via NHSmail.

2.2.4 Confidential information must not be sent to share or group email boxes (unless all those with access to the mail box have the necessary security authorisation and access).

2.2.5 Confidential information must not be forwarded by e-mail to any person or organisation that is not specifically authorised to review and view that information.

3.0 Safe Haven Incoming and Outgoing Post

3.1 **Do's for Incoming Post**

3.1.1 Deliver incoming post efficiently and quickly to the recipient. If the recipient is unavailable the designated deputy must take responsibility for the post.

3.1.2 If the post is marked "Private and Confidential" to a named recipient, only the named recipient should open the post (unless prior arrangements have been agreed).

3.1.3 If the named recipient is known to be absent for a period of time post should be redirected to the Team Manager.

3.1.4 Any confidential post, not immediately given to the recipient, must be locked away until they can receive it. The holder of the information is responsible for it until it is handed over to the recipient.

3.1.5 Once the post has been passed over, it is the owner's responsibility to ensure the safe keeping of the confidential information, using their own safe haven locked cabinet / room / drawer (see notes on storage of information).

3.1.6 A return address must be printed clearly on the internal postal envelope to ensure the post can be sent back to the original sender if received in error by the wrong recipient.

3.2 Do's for Outgoing Post

3.2.1 Make sure outgoing post is addressed to the correct recipient.

3.2.2 When sending confidential information to another organisation always mark with "Private and Confidential – To be opened by Addressee only". The recipient's name and full postal address should be clearly **printed** on the envelope or a window envelope used. This information should only be sent by 1st class post and NOT 2nd class post.

3.2.3 Include a return address to ensure that if the envelope is received in error, the recipient can return the post without opening the envelope.

3.2.4 For clinical information consider addressing to the 'Team' rather than an individual, if appropriate and depending upon the urgency of the correspondence.

3.2.5 When sending mail that is confidential but to a number of people, e.g. a team or service, the correspondence and the envelope should be clearly marked "Private and Confidential".

3.2.6 Sensitive person-identifiable information should only be sent by "Recorded / Special Delivery" service, which includes both a Track and Trace and an electronic Proof of Delivery (ePOD) facility, so that the location of the package can be determined through its journey, and the final delivery signature checked (e.g. Special Cases, Health Records, Child Health Records, etc). appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the name and full postal address of the recipient is Printed clearly on the package or written in permanent marker using block capitals on a plastic document wallet.

3.2.7 Where there are several packages / particularly large packages the sender may need to consider the use of authorised courier services (advice on authorised courier services can be obtained from the Trusts Records Manager). It is

essential to confirm that the courier service has tracking systems in place, including recording of collection / delivery and traceability of the package.

3.2.8 When sending confidential information to another organisation you must stamp or mark the envelope:

SAFE HAVEN
Private and Confidential / Addressee Only
If undelivered, please return to sender:
(Sender's address – use the designated PO Box number for your site)

3.2.9 Post intended for patients, residents, their relatives or carers should not have any Trust identifiable return address / franking marks on the envelopes in order to maintain the confidentiality of that person (**use the designated PO Box number for your site**). It is noted that this is not always under the control of the Trust where post is handled on the Trust's behalf by other organisations.

3.2.10 Teams should undertake risk assessments on the types of correspondence they send to assess which correspondence would need to be sent "Recorded / Special Delivery". Highly sensitive information (e.g. full assessment reports / sensitive person information, e.g. health or physical condition, sexual life, ethnic origin, religious beliefs, political views or criminal convictions) may need to be Recorded / Special Delivery whereas, e.g. an appointment letter, containing minimal personal information could be sent by normal postal services.

3.2.11 When sending confidential information using the internal post, ensure that the information is placed in a sealed envelope and then placed in the transit envelop with "Private and Confidential" written on the outside.

3.2.12 Call the recipient to ensure the confidential information has arrived or ask the recipient to call when they have received the confidential information, where appropriate.

3.3 Don'ts for Outgoing Post

3.3.1 Leave confidential post unattended in an open area.

3.3.2 Send confidential information to insecure locations.

4.0 Safe Haven Verbal Communications, Phones and Answer Phones

4.1 <u>Do's</u> for verbal communication, phones and answer phones

4.4.1 Try not to disclose confidential information over the phone because of risk involved (e.g. being overheard, inadvertent disclosure of confidential information, disclosing confidential information in an inappropriate manner, etc.).

4.4.2 Try to have phones away from the reception area. If this is not practical, take reasonable steps to protect a patient's/residents/ client's or the organisation's confidentiality whilst speaking on the phone.

4.4.3 Ask questions over the phone that require the patient/resident or client to answer rather than giving them details which they need to confirm e.g. try not to say “Is that Joan Bloggs of 15 Town Road, Any Town?”. Instead ask the patient/resident or client who they are and where they live and do not repeat the information out loud.

4.4.4 If you receive a call from another health professional, confirm their identity and their reason for asking before giving out any confidential information.

4.4.5 If you have any doubt as to the identity of the caller, call them back using a published telephone number (rather than one they quote).

4.4.6 Put callers on hold so they cannot hear other confidential conversations that may be going on in the office.

4.4.7 In face to face situations ask for proof of identity and once verified ensure that discussions take place in private locations and not public areas, common staff areas, lifts etc.

4.4.8 It is vital that the correct patient/resident is being discussed. The wrong information may be given out if there is a misunderstanding so make sure first.

4.4.9 If you receive a call from someone claiming to be a relative and asking information relating to the condition of the patient or resident, check with the patient person for permission (consent) to disclose. Until you have this permission (consent) you must not confirm or deny whether you have a patient or resident with that name so that you do not breach confidentiality. If this is not possible then do not disclose any information.

4.1.10 If the Police request any patient or resident identifiable information they should be directed to the Head of Records Management / Legal Manager.

4.1.11 Media requests for patient or resident identifiable information must always be referred to the Trust DPO/ Records Manager or Information Governance Manager. Staff are not authorised to release any identifiable information to the media or press.

4.1.12 Ensure before information is given out that the enquirer has a legitimate right to have access to the information.

4.1.13 Ensure answer phones are located in a secure area and are only accessible by authorised personnel.

4.1 <u>Don’ts</u> for verbal communication, phones and answer phones

4.2.1 Repeat any confidential details that a patient/resident gives you if others may hear them e.g. there is no need to mention forenames and surnames out loud in the same conversation.

4.2.2 Have the phone switched on to “speaker” mode, turning a confidential call into a “tannoy” message.

4.2.3 Assume permission (consent) if you are asked to give patient /resident information to a relative – check with the patient/resident or your manager first.

4.2.4 Leave messages containing confidential information on answering machines unless permission (consent) has been given to do so.

4.2.5 Leave messages containing confidential / sensitive information on white boards / notice boards.

4.2.6 Do not store staff personal numbers on the phone particularly if it is in a shared area or office.

5.0 Safe Haven Information Storage

5.1 **<u>Do's</u> for information storage**

5.1.1 Ensure all confidential information is stored in locked cabinets / rooms / drawers. There are designed safe havens for confidential information. A clear desk procedure should, where possible, be in place.

5.1.2 All sensitive records must be stored face down in public areas and not left unsupervised at any time.

5.1.3 When information needs to be removed for use, make a record of when it was removed and by whom. The person removing the information is then responsible for maintaining its confidentiality and returning it to the locked cabinet / room / drawer (or their own) as quickly as possible.

5.1.4 Keep a note if any information is transferred so that it can be tracked if necessary.

5.1.5 Continually assess whether information needs person identifiers or whether it can be anonymised.

5.1.6 Nominate a person to be responsible for holding the keys to the locked cabinets / rooms / drawers. This person will be responsible for the safe-keeping of the information within the cabinets / rooms / drawers.

5.1.7 Audio tapes or CD's awaiting text should be kept in a locked cabinet / room / drawer and erased immediately after use.

5.1.8 Protect confidential information by encryption (or other Trust approved protection methods) and strong authentication.

5.1.9 Only transfer confidential information in accordance with Trust approved policies and procedures.

5.1.10 Store confidential information on the Trust network servers, in restricted access folders (refer Information Governance and Security Procedure and Procedures)

5.1.11 Only use authorised and encrypted laptops / ipads to process confidential information. The level of protection that the encryption provides must meet the

minimum as laid down by the Department of Health and Connecting for Health guidelines in relation to the electronic transfer of person identifiable information / confidential information.

5.1.12 The laptops / ipads should also be configured with anti virus / anti-malware software, which is active.

5.2 **Don'ts for information storage**

5.2.1 Copy to or hold information on removable media (e.g. USB devices, laptops, ipads, portable hard drives, Blackberry mobile phones etc.), unless it is absolutely necessary or has been authorised. Only use encrypted removable media issued / approved by the Information Governance Team or ITT Team. Personally owned removable media must not be used in any circumstances.

5.2.2 Leave any approved removable media (e.g. USB devices, laptops, ipads, dictaphones or portable hand held drives etc.) containing sensitive / person-identifiable information accessible or in view.

5.2.3 Label the approved removable media (e.g. USB devices, laptops, ipads, portable hard drives etc.) in any way which might identify that the device holds confidential information.

5.2.4 Upload any incoming removable media (e.g. USB devices, laptops, ipads, portable hard drives etc.) from other organisations until the security has been checked by the anti-virus.

5.2.5 Hold any confidential information on local drives (C:// Desktop or My Documents, My Pictures, My Videos, etc.). (Only store this information on Trust network server(s), in restricted access folders).

5.2.6 Leave confidential information unattended at any time.

5.2.7 Leave documents unattended at the photocopier if person identifiable information is present.

5.2.8 Leave confidential information in any area where it may be seen or looked at by unauthorised persons, even for short periods.

5.2.9 Leave files open when not in use.

6.0 Safe Haven Shredding

6.1 **Do's for shredding**

6.1.1 Destroy confidential information in a correct way. Use a **cross-cutting** shredder for the destruction of confidential information.

6.1.2 Make sure everyone knows how to use the cross-cutting shredder and what type of information should be destroyed using it.

6.1.3 Make sure that records are kept for the specified length of time. (Department of Health: NHS Records management – Code of Practice Parts 1 & 2) and then shredded.

6.1.4 Treat surplus or spoiled photocopies of confidential information as confidential waste.

END

Essex Partnership University
NHS Foundation Trust

SAFE HAVEN PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG50C
VERSION NUMBER:	6
KEY CHANGES FROM PREVIOUS VERSIONS:	3 year review; fax guidance amended to pharmacy use only
AUTHOR:	Information Governance Team
CONSULTATION GROUPS:	Policy Steering Group, Information Governance Steering Sub-Committee Key Information Governance Leads
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	Aug 18 (GDPR); May 2021
LAST REVIEW DATE:	May 2021
NEXT REVIEW DATE:	May 2024
APPROVAL BY INFORMATION GOVERNANCE & SECURITY SUB-COMMITTEE:	April 2021
RATIFICATION BY QUALITY COMMITTEE:	May 2021
COPYRIGHT	

PROCEDURE SUMMARY

These procedural guidelines will ensure that all staff are aware of the use of Trust systems in regard of patient, staff, general wider public information / data that occurs and which ensures that processes are in place to protect, highlight actual or potential confidentiality breaches in systems.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this procedure, 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 policy is The Executive Chief Finance Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SAFE HAVEN PROCEDURE

CONTENTS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SAFE HAVEN PROCEDURE

Assurance Statement

This procedure aims to ensure that wherever and whenever person identifiable information (patients/staff and/or the public) flows to and from the Trust, those persons responsible for transmitting and receiving it are fully aware of Safe Haven principles and procedures.

These procedure guidelines should be read in conjunction with other relevant trust policies and procedures (see 4.0).

1.0 INTRODUCTION

1.1 The need to ensure that confidential information is safeguarded is a major concern to all staff working within the NHS. The NHS has an enviable reputation for maintaining the confidentiality of personal health information, which it acquires for the purpose of clinical care, patient administration medical records management, wider management and planning, teaching and training, disciplinary proceedings and research.

1.2 Although the term "Safe Haven was originally implemented to support contract procedures it is now recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of patient identifiable/confidential information / documentation between organisations or sites using different forms of media (e.g. post, e-mail, telephones, answer phones, computer systems, electronic media, manual records, books, whiteboards and notice boards).

1.3 Person identifiable / confidential information / documentation may include information on staff, patients, companies and / or the wider general public.

1.4 Sensitive (special) Personal Information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community (e.g. health or physical condition, sexual life, ethnic origin, religious beliefs, Trade union, political opinions, criminal convictions).

1.5 Business Sensitive Information is information that, if disclosed, could harm or damage the reputation or image of an organisation.

1.6 A Safe Haven is any location that is used to send and receive identifiable / confidential information in a NHS organisation securely and confidentially. Any computerised or manual document that personally identifies a person (e.g. name, address, postcode, age, gender, payroll / hospital number, bank details, voice and visual records etc.) is classed as confidential.

1.7 A Safe Haven may be either a secure physical location or the agreed set of administrative arrangements that are in place within an organisation to ensure identifiable / confidential information is communicated safely and securely.

1.8 The Trust and its employees must ensure that wherever and whenever information flows to and from the Trust, those persons responsible for transmitting and receiving it are fully aware of safe haven principles and procedures and that they adhere to them.

1.9 The following principles detail routine practice for the transfer of person identifiable (confidential) information to and from the Trust.

1.10 Patient Health Records, other paper / electronic records, correspondence and all data should always be kept in a secure fashion.

2.0 GENERAL GUIDANCE

2.1 When sending or receiving information Trust staff must be confident that they are not breaching or compromising confidentiality.

2.2 Personal identifiable information should not be given, posted, faxed, emailed or discussed with anyone other than those who specifically need it and are authorised to have access to it.

2.3 For any forms of requests (telephone, e-mail, letter, memorandum and/or face to face etc.) where there is uncertainty about the ethics of passing on information staff should seek advice from Line Managers and / or the Trust's Information Governance Manager or Trust DPO.

2.4 Details of the Trust's Information Governance Manager or DPO can be found on the Intranet.

2.5 Staff should be aware that the use of unique identifiers, such as the NHS Number, does not negate the need to follow these procedural guidelines.

2.6 If a safe haven room / area is on the ground floor any windows should have locks on them.

3.0 SCOPE AND PURPOSE

3.1 Scope

3.1.1 This document aims to set out the practical guidance to ensure that all transfer of person identifiable / confidential information is undertaken according to the Caldicott / Data Protection Principles.

3.1.2 This procedure is designed to be disseminated to all staff to ensure that they are aware of their responsibility to comply with the NHS Safe Haven Procedure.

3.1.3 This procedure will be reviewed periodically to keep pace with future developments arising from changes in the organisation and management of the NHS, the application of the Data Protection Act 2018, the Freedom of Information Act and other legislation.

3.2 Aims & Purpose

3.2.1 To ensure that the Trust has a Safe Haven Procedure in place and that it is communicated to all staff, so they are aware of their responsibilities when handling identifiable information and act in accordance with this procedure.

3.2.2 The purpose of this procedure is to provide:

- A definition of the term safe haven
- Advise when a safe haven is required
- The necessary procedures and requirements needed to implement a safe haven
- Rules for different kinds of safe haven
- Guidance on who can have access and who you can disclose to

3.2.3 Such procedures are required to:

- Ensure that all staff who handle information are aware of their responsibility to ensure that information remains secure and confidential at all times
- Ensure that all handling of confidential information only takes place on an strict need to know basis and only as a part of his / her legitimate activity to undertake his / her job roles in the interest of patient care
- Ensure that all staff members who are authorised to handle patient information are aware of their duty to understand the Law and comply with it.
- Ensure that all written transfers should be limited to those details necessary in order for the recipient to carry out their role.

4.0 SAFE HAVEN PROCEDURES

4.1 Please refer to Appendix 1 and Appendix 2 for the “do’s and don’ts” on how to send information by the following methods;

Fax is currently only permitted for use by Trust Pharmacy services.

4.1.2 ***Electronic information (transfer by email)***

4.1.2.1 Email transmission over networks can have serious risks. Transfer of confidential information must be avoided unless essential to the delivery of Healthcare. Where authorised email has to be used, this must follow Trust procedure, guidance and good practice.

4.1.2.2 If patients / staff have specifically consented to communication via email, consent should be obtained in writing and held on the

person's health / staff record. Only sending of information of a general nature is then permitted.

4.1.2.3 Microsoft Outlook – Although this is managed and protected by the Trust's networks, staff are not permitted to send confidential personal identifiable or Trust sensitive information via this method, external to the Trust, unless email encryption is available and used or are sending NHS.net to NHs.net.

4.1.2.4 It is the responsibility of individual staff / teams to decide whether to send other types of confidential information. Staff must arrange a document password protection with recipients if they need to send confidential documents on a regular basis. The sending of information of a general nature is permitted.

4.1.2.5 If you receive a misdirected email inform the sender so that they can resend it. Delete the email from your system (including the "deleted" box). And raise a Datix.

4.1.2.6 **Contact Centre (Only)**

In order for the Contact Centre to provide an efficient service, it must be advised on a daily basis of staff movements. Emails will be sent to the Contact Centre by teams / services to update on daily sick, study, annual leave, etc. The header for these emails should contain the wording "Daily Update" the email will be sent nhs.net to nhs.net which is a secure transfer but will still only contain the required information needed for the service to continue e.g.

- Name of person (initial and surname, e.g. J Smith)
- Location (work base, e.g. Harland)
- Reason for absence using the positive return codes (e.g. for sick leave SS)
  (Example: J Smith, Harland, is absent SS – do not send emails/texts)

4.1.3 ***Incoming and outgoing post***

4.1.3.1 Always remember to mark outgoing post correctly. Include the recipient's name and correct address.

4.1.4 ***Verbal communications, phones and answer phones***

4.1.4.1 Disclosures of confidential information to anyone unknown is strictly forbidden.

4.1.4.2 When a health professional / manager makes an entry in a shared record, it is on the understanding that all those with access to the record will respect the duty of confidentiality and will not disclose any of the record content without the appropriate permission (consent).

4.1.5 ***Information storage***

4.1.5.1 Keep information secure and confidential at all times.

4.1.6 ***Shredding***

4.1.6.1 Only cross-cut shredders are allowed to be used.

5.0 SHARING INFORMATION WITH OTHER ORGANISATIONS (NON NHS)

5.1 Employees of the Trust authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving confidential information.

5.2 The Trust must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements.

- Data Protection Act 2018
- Common Law Duty of Confidence
- NHS Code of Practice: Confidentiality
- Human Rights Act 1988
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- NHS Code of Practice: Information Security
- General Data Protection Regulation

This list is not exhaustive and staff will be required to implement / take regard of any new / updated legislation as it arises.

5.3 Staff sharing confidential information with other agencies should be aware that Information Sharing Protocols and agreements need to be drawn up when sharing information, please contact the Information Governance Team for further advice. (Refer to Information Sharing Procedure)

6.0 REFERENCE TO OTHER DOCUMENTATION

6.1 These procedural guidelines should be read in conjunction with:

- Sharing Information and Consent Policy / Procedure
- Data Protection and Confidentiality Policy / Procedure
- IM&T Security Policy / Procedure
- Records Management Policy / Procedures
- IT Security Policy
- Freedom of Information Policy / Procedure
- Information Governance and Security Policy / Procedure
- NHS Code of Practice: Confidentiality
- Human Rights Act 1988

- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- NHS Code of Practice: Information Security
- NHS Caldicott Principles
- Access to Health Records

This list is not exhaustive and staff will be required to implement / take regard of any new / updated legislation affecting records managements as it arises.

7.0 STAFF TRAINING

7.1 All staff working for the Trust must attend a mandatory training session on Information Governance by completing the E-Learning tool. Information Governance training is an annual requirement.

8.0 COMPLIANCE

8.1 Compliance with this procedure will be monitored through the Trust's procedure compliance programme and through spot check audits carried out by the Head of Records Management and the Information Governance Manager.

8.2 Ensure any potential breaches are reported via the Head of Records Management / Information Governance Manager and appropriately recorded via the Trust's information incident reporting system (Datix).

8.3 Any incidents reported using the Trust's incident reporting process will be monitored to identify breaches to this procedure and such incidents will be investigated. Staff should be aware that failure to comply with the safe haven principles could result in disciplinary action.

END

INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE - CPG50(D)

(March 2016)

APPENDIX 1

~~SOUTH~~ ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SECURITY INCIDENT OPENING REPORT FORM

SECURITY / CONFIDENTIALITY BREACH INCIDENT NO…… (*to be completed by the Information Governance Department*

Department: ……

Directorate: ……

Location/Site: ……

Reporting Officer(s): ……

Telephone Number: ……

Incident Reported to: ……..

Date Reported: ……..

Incident Date: ……
(if known, else approximate)

Incident Description:

APPENDIX 2

~~SOUTH~~ ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION SECURITY INCIDENT INVESTIGATION FORM

SECTION A Incident Details

DETAILS OF INCIDENT:

Date of incident:

Service area / Site:

Staff involved:

Patient/Resident(s) involved:

Others involved:

Please indicate the area(s) of impact of this incident as appropriate:

IT Equipment / Systems Failure (inc. hardware/software)	☐
System Infiltration / Computer Misuse / Abuse	☐
Confidentiality Breach	☐
Theft or loss	☐
Unauthorised Access to Area	☐
Error by Personnel	☐
Malicious Act	☐

Type of Breach:

- ☐ **Patient Related**
- ☐ **Staff Related**
- ☐ **Sensitive Data**
- ☐ **Corporately Sensitive**
- ☐ **Other (specify:**

(if more than one category applies, indicate which one was the first cause)

INVESTIGATION:

Investigating Officer:
(Name)

(Designation)

(Contact Details)
Phone:
Mobile:
Email:

AIR Form / Datix No:
(If applicable)

INVESTIGATION INTERVIEWS:

Interview 1:

Date of Interview:

Name of Person Interviewed:

Designation of Person Interviewed:
(e.g. Patient, Resident, Staff [title], Visitor, etc.)

Interview 2:

Date of Interview:

Name of Person Interviewed:

Designation of Person Interviewed:
(e.g. Patient, Resident, Staff [title], Visitor, etc.)

(Repeat Interviews as necessary)

FINDINGS / CONCLUSIONS & RECOMMENDATIONS:

Findings / Conclusions:

Recommendations:

Signed:
(Investigating Officer)

Date:

CPG50D - Appendix 3

INFORMATION SECURITY INCIDENT REPORTING PROCESS

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

An information security incident (Incident) / information confidentiality breach (Breach) is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the computer system or data being put at risk
- The availability of the computer system or information being put at risk
- An adverse impact, for example:

  a) Threat to personal safety or privacy;
  b) Legal obligation or penalty;
  c) Financial loss;
  d) Disruption of Trust business; or
  e) An embarrassment to the Trust.

All staff have a responsibility for reporting security Incidents / Breaches.

The Trust's Executive Chief Finance Officer (Senior Information Risk Owner) and the Executive Medical Director (Caldicott Guardian) are the Directors responsible for information security / confidentiality and with the Information Governance Manager are responsible, for implementing, monitoring, documenting and communicating information security within the organisation, in compliance with all UK legislation and national policy and guidance.

The Data Protection Officer and the Information Governance Manager are responsible for:

- Monitoring and reporting to the Chief Executive (SIRO) the state of information security within the Trust;
- Developing and enforcing detailed policy and procedures to maintain security and ensuring that these are implemented throughout the Trust and followed;
- Ensuring compliance with relevant legislation, including the General Data Protection Regulation and Data Protection Act 2018;
- Ensuring that relevant staff are aware of their security / confidentiality responsibilities and that security awareness training is provided for all IT users;
- Monitoring for actual or potential information security / confidentiality breaches within the Trust.

Trust management also has a responsibility to ensure that staff are aware of security risks and their responsibilities to minimise threats, i.e. Management should:

- Ensure that all current and future staff are instructed in their security responsibilities;
- Ensure that all staff using computer systems are trained in their use;
- Ensure that no unauthorised staff are allowed to access any of the Trust's computer systems as such access could compromise data integrity;
- Determine which individuals are to be given authority to access specific computer systems. The level of access to specific systems should be on a job function, independent of status;
- Implement procedures to minimise the Trust's exposure to fraud / theft / disruption of its systems, such as segregation of duties / dual control / staff rotation in critical susceptible areas;
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability;
- Ensure that staff are aware of the Trust's Standing Orders on potential personal conflicts of interest;
- Ensure that all staff sign confidentiality (non-disclosure) undertaking as part of their contract of employment; and
- Ensure that the relevant systems managers are advised immediately about staff changes affecting computer access so that passwords may be withdrawn / deleted.

Overview of reporting

All incidents / breaches or information indicating a suspected (near miss) or actual security breach should initially be reported to the immediate line manager.

The majority of breaches are innocent and unintentional (e.g. user not 'logging out' when leaving for the day) and would not normally result in disciplinary action being taken.

All incidents whether they are actual or near misses must reported by staff within 24 hours of the incident using the appropriate web based Datix Incident Reporting Form. The Information Governance Team will determine whether an actual breach has taken place.

The Information Governance Team will categorise the incident / breach within one of the classifications (from insignificant to acute) as defined in the Risk Matrix found in the CPG50D Procedure.

Where an incident / breach has occurred the Information Governance Team will report to the ICO.

All incidents / breaches that may have an impact on NHS.net will be reported immediately, by the Information Governance Team, to the

Regional Telecommunications Branch Security Coordinator or NHS.net Security Manager.

The information Governance Team shall maintain a record of all reported incidents / breaches which will be reported to the Trust Board and Caldicott Guardian at regular intervals.

Reporting Procedures if Datix is available for use.

Datix is a dedicated risk management software that provides a joined up approach to risk management and compliance against standards by bringing together Incident Reporting, Complaints, Claims, CQC Standards and Risk Registers. The link for Datix can be accessed via the Trust's intranet home page.

What to expect from the incident reporting form:

The form itself is simple and is structured systematically enabling you to identify the type of incident, location, category, and contacts. All sections with a red star are mandatory and require an entry. The form has several drop-down boxes giving you a number of options to choose from.

Incident date and time:

A calendar will appear and this will allow staff to choose the date the incident happened and enter a time format using a 24-hour clock.

Area:

This option will allow staff to identify which area the incident relates to.

What is the name of your team, where your team is based, which service / specialism are you reporting from:

These options will allow staff to choose which team / service / specialty which contributed towards the incident or may have been involved in an incident which was committed by an external organisation. Identifying the service / specialty will allow the service / specialty lead to be notified that the incident has occurred.

Where did the incident occur (location), at what type of location did the incident occur:

These options will allow staff to enter the location where the incident occurred and what types the location might be (e.g. GP Practice, car park etc.).

Describe what happened, immediate action taken:

These options will allow staff to detail the events of the incident and what action the staff member reporting the incident might have taken or the staff member's line manager or the patient / service user / external organisation might have taken. (Note: No names, initials or place names should be used in these sections)

Incident classification, Additional information, Persons involved, Details of the reporter, Name of Manager

The above section will allow staff to add the incident type (e.g. Security, Procedures, Breach of Confidentiality etc.) and any additional information which might be relevant to the reporting process. Details of persons related to the incident need to be entered to allow the investigating officer the option to contact these persons when necessary to ensure the investigation is done correctly and according to policy.

(Note: For any queries or comments about the e-Form, please contact the Risk Management Department)

Reporting Procedures if Datix <u>is not</u> available for use.

An unusual incident or significant security breach must be reported on an Incident Opening Form (see Appendix A). The form must be completed by either the Reporting Officer or their line manager and forwarded to the Risk Management Department.

The Information Governance Team are responsible for ensuring that the Incident Opening Form is completed where deemed appropriate and that, at the same time, an Incident Investigation form is opened (see Appendix B).

The Information Governance Team must maintain a log of all Incident Opening and Investigation forms completed.

Incidents must remain open until the 'Cause and Action' section of the incident investigation form is completed to a satisfactory conclusion. As soon as is possible during the course of the investigation the Information Governance Team must categorise the incident / breach within one of the categories (from Insignificant to Acute) as defined in

the Classification of Incident table in Appendix C. The incident / breach may need to be re-categorised during the course of the investigation as new information or impacts are discovered.

If the security breach is defined as Significant, Major or Acute then the SIRO / Caldicott Guardian must be informed immediately and fully briefed at the first opportunity.

Where the incident / breach impacts on the Trust's computer, network, server delivery the Information Governance Manger is responsible for fully briefing the Associate Director of IT and / or the Associate Director of Electronic Systems and IG on all aspects of a Significant, Major or Acute incidents / breaches.

Any staff member reporting a breach of IT security must have unhindered access to the Associate Director(s) of Electronic Systems and IG if that staff member believes the breach has been as a result of an action by the Information Governance Manager.

The Information Governance Manager is available to any member of staff reporting a breach in information security. The anonymity of the member of staff must be ensured, irrespective of whether or not the event turns out to be a genuine breach or a false alarm. It is most important that the reporting process is made as easy as possible, especially where the offence is being committed by someone in a position of trust. It is possible that the offender may be in a position of authority over the staff member making the report. Therefore, it is essential that no adverse pressures are brought to bear on the staff member as a consequence.

The Information Governance Team are responsible for ensuring that documented records of incidents are retained and stored securely for audit review.

Essex Partnership University
NHS Foundation Trust

INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

POLICY REFERENCE NUMBER:	CPG50d
VERSION NUMBER:	3.1
KEY CHANGES FROM PREVIOUS VERSION	Amendments – s5.4 expanded, s7.7 added
AUTHOR:	Alice Williams Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub-Committee. Quality Committee.
IMPLEMENTATION DATE	June 2019
AMENDMENT DATE(S)	October 2019 (ID no. Change); Sept 2021; June 22 (actioned Dec 22)
LAST REVIEW DATE	September 2021
NEXT REVIEW DATE	September 2024
APPROVAL BY IGSSC	August 2021
RATIFICATION BY QUALITY COMMITTEE	September 2021
COPYRIGHT	© 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

PROCEDURE SUMMARY

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.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

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

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this policy is The Senior Information Risk Officer

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION GOVERNANCE INCIDENT REPORTING PROCEDURE

CONTENTS

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

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.

- 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

- 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.

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. A Service User's Clinician must be engaged in the decision on whether or not to disclose an incident to a patient. If the clinician, after reviewing the patient's record, believes it is not of overall benefit to the individual to disclose an incident involving the loss or breach of personal information or being informed of the incident could cause harm to the individual's wellbeing or Mental Health, the clinician may recommend that the incident is not disclosed. If it is decided not to disclose, this must be recorded in the patient record and include reasons for the decision. There must be a justifiable decision.

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.

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?

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.

7.7 When deciding whether to inform a service user of the loss or breach to their data, you must consider;

a. the potential harm or distress to the patient arising from the disclosure
b. future engagement with treatment and their overall health
c. the potential harm to trust in doctors generally
d. the nature of the information that has been disclosed

Due to the above it is imperative that the clinician involved in the care of the individual is contacted and the incident is discussed.

You must document in the patient's record your reasons for not informing the service user. You must also document any steps you have taken to reach this decision.

Decisions about whether or not to disclose can be complex.

You can also seek advice from the Trust Caldicott Guardian, Data Protection Officer or the Information Governance team. If possible, you should do this without revealing the identity of the patient.

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'.

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.

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.

					DHSC & ICO		
Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
					ICO		
	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-coordinating 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 Trust wide in the staff Wednesday Weekly Communication Articles.

END

Essex Partnership University
NHS Foundation Trust

DATA PRIVACY IMPACT ASSESSMENT PROCEDURE

(Implementing new Software, Hardware, Processes & Systems)

PROCEDURE REFERENCE NUMBER:	CPG50e
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	Three year review; New Excel DPIA tool to replace Word version
AUTHOR:	Alice Williams Information Governance Manager
CONSULTATION GROUPS:	Information Governance Steering Sub Committee
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2023
LAST REVIEW DATE:	March 2023
NEXT REVIEW DATE:	March 2026
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	December 2022
RATIFICATION BY POLICY OVERSIGHT & RATIFICATION GROUP:	March 2023
COPYRIGHT	

PROCEDURE SUMMARY
These procedural guidelines and their associated policy document will ensure that the introduction of new / changes to software, hardware, systems and processes are assessed for privacy impacts in line with national guidance to prevent breaches of confidentiality, in relation to person identifiable information prior to them being installed / implemented.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
Compliance with the DPIA requirement is monitored by the IG Team, which regularly reviews incidents reported on Datix to establish if they have been caused in whole or part by DPIAs not being appropriately completed. To ensure projects appropriately complete DPIAs, there will be IG membership / attendance / review of minutes at the Trust's various project groups.

Services	Applicable	Comments
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PRIVACY IMPACT ASSESSMENT PROCEDURE
(Implementing new Software, Hardware, Processes & Systems)

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Data Privacy Impact Assessment Procedure

Assurance Statement

These procedural guidelines and their associated policy document will ensure that the introduction of new / changes to software, hardware, systems and processes are assessed for data privacy impacts in line with national guidance to prevent breaches of confidentiality, in relation to person identifiable information prior to them being installed / implemented.

1.0 INTRODUCTION

1.1 The Trust undergoes change on an on-going, regular basis and rapidly changing technology and these changes although often simply to keep up to date with safe and secure processing of information can have a major impact on the confidentiality of that information.

1.2 A Data Privacy Impact Assessment (DPIA) is a process which helps assess privacy risks to individuals' data in the collection, use and disclosure of information. They help identify privacy and / or corporately sensitive data risks, foresee problems and bring forward solutions.

1.3 DPIAs must be conducted by someone that is introducing a new or significantly changed project, procurement, business case or departmental/team initiative that involves Personal Identifiable Data (P.I.D). The responsibility for carrying out the DPIA must be formally recorded and assigned by the Project Board / appropriately senior Manager

The Project Manager or Board (however these are defined, depending on the size of the project) must proactively consider how project management activity can address privacy issues. These must also be discussed with all appropriate stakeholders

1.4 These guidelines detail the process to be followed to assess new / changes to systems / processes to determine whether person identifiable / corporately sensitive information is collected / utilised within the new system / process.

1.5 These guidelines must be followed by any staff / project team involved in the design / development of new / changes to systems / processes and where changes to hardware / software / processes are required. Privacy implications must be considered at each phase of the life-cycle of a project. This may result in several DPIAs being completed or updated. It is for the Project Manager or Board to ensure this is effectively managed.

1.6 Answering a set of screening questions within the DPIA document will identify if there is any potential impact on privacy. A positive answer to **any** of the questions confirms that a Full DPIA is required.

1.7 When a DPIA is completed it must first be reviewed by the appropriate Project Board, and then be submitted to the Information Governance Team by email for processing.

For patient-based DPIAs, the IG Team will make a recommendation to the Caldicott Guardian, who acts as the Trust's conscience with regard to use of patient information and has ultimate sign-off for the processes using their information. For similar non-patient based DPIAs, such as (but not limited to) Human Resources, the sign-off will be undertaken by the Trust's SIRO. The recommendations will be either Approved or Declined.

Once approved by the IG Team DPIA Panel and passed through the Cyber Security Manager, IT Manager and the Data Protection Officer (DPO) or their Deputy it will then be sent on to the Caldicott Guardian / SIRO (as applicable), who will Approve or Decline it.

This process will continue cyclically until such time as the IG Team and Caldicott Guardian / SIRO (as applicable) are in agreement with the project's proposals.

DPIAs must be retained by the Project Board / appropriate Senior Manager and form part of official Project Documentation where applicable.

2.0 SCOPE

2.1 These procedures must be adhered to by all staff / services / project teams intending to install new / changes to systems and / or implement process change.

2.2 The Information Asset Owner (responsible manager for the information / data) will have overall responsibility for completing the PIA.

3.0 RESPONSIBILITIES

3.1

Role	Responsibility
Information Governance Steering Sub-Committee	o Accountable for the DPIA outcome and risks
Lead	o Responsible for the completion and follow-on actions identified within the DPIA o Responsible for assigning appropriate owners of risks identified within the initial screening questionnaire and subsequent DPIA
Project Manager	o Accountable for the completion of the initial screening questionnaire with the relevant person. o Responsible for forwarding draft/completed DPIA's to the IG Manager for advice and comments. o Responsible for the electronic storage of completed DPIA once approved.

	o Responsible for the: o completion of the Project Brief and Overview o completion of the initial screening questionnaire o inclusion of the status and outcome of screening questionnaires to the appropriate Project Board o management of any risk identified by the initial screening questionnaire and subsequent DPIA
IG Manager/DPO	o Responsible for the communication of screening questionnaires to the IG Steering groups o Accountable for the DPIAs (Full and Small Scale) where identified by the initial screening questionnaires
IG Team	o Provide quality assurance of the completed screening questionnaire. o Responsible for the communication of screening questionnaires to the IG Steering groups o Accountable for the DPIAs (Full and Small Scale) where identified by the initial screening questionnaires

3.1.2 Following the DPIA assessment the IG Team will be responsible for presenting the outcome of the DPIA to the appropriate Committee for approval and for ensuring that the Senior Information Risk Owner / Caldicott Guardian is made aware of any significant risks / outcomes which may need escalation to the Information Governance Steering Committee.

4.0 AIMS AND OBJECTIVES

4.1 The Trust requires DPIA's to be undertaken for the following reasons:

- Identifying and managing information risks – DPIA's are part of good governance and risk management
- Avoiding unnecessary costs – by performing DPIA's at the earliest stage of a new project or process change potential problems can be identified which would minimise extra costs at a later stage
- Inadequate solutions – DPIA's can make a project / process change more resistant to failures around individual privacy – it will also facilitate recovery in the event of failure
- Avoiding loss of trust and reputation – DPIA's will ensure systems / processes will not be deployed with privacy flaws which may ultimately attract the attention of the media, public, or regulators
- Informing the organisation's communications strategy – the use of DPIA's to inform relevant stakeholders of impending new systems / processes will ensure that all stakeholders have the opportunity to discuss and review the privacy impact of those new systems / processes

- Meeting and exceeding legal requirements
- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- Where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them.
- Documentation of the outcomes

5.0 PROCEDURES

5.1 DPIA's should be carried out at the start of a new system installation, process change and / or hardware / software implementation.

5.2 To achieve optimum identification of possible risks to a system / process change the following guidance should be followed:

- Start the screening process early (e.g. at the project initiation phase) to ensure that project risks are identified and appreciated before the problems become imbedded in the design (e.g. at the start or as near possible, of the project / system / process / hardware or software change.

5.3 The nominated assessor (identified by the Information Asset Owner as the person with overall responsibility for the project, system/ process change) will complete the DPIA screening tool, Appendix 1

5.4 The screening tool may identify that no person identifiable information / privacy intrusive information is being handled as part of the project, system / process change. In this case a copy of the DPIA should be sent to the Information Governance Team who will advise whether any further action is required / approve accordingly.

5.5 Where the screening tool has identified that person identifiable / corporately sensitive information / privacy intrusive information is being handled the completed tool (DPIA) should be forwarded to the Information Governance Team who will ascertain whether all data protection issues have been considered, make recommendations where necessary, and forward the DPIA

to the necessary Committee (usually the Information Governance Steering Sub-Committee) for approval.

5.6 Once the final DPIA has been presented and agreed / recommendations made by the appropriate Trust Committee / Group the IAO will be notified by the Information Governance Team to ensure changes can be implemented.

6.0 SUPPORT

6.1 The Trust's Information Governance Team will be available to support all staff who are required to undertake a DPIA assessment.

6.2 The timescales for ratification of a DPIA are included in Appendix 1

7.0 MONITORING AND REVIEW

7.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

7.2 Compliance to this policy and procedural guidelines will be undertaken in line with Trust policy and timetables for compliance audits.

7.3 The Information Governance Group / Caldicott Network will have overall responsibility for overseeing the implementation of these procedural guidelines.

7.4 Compliance with the DPIA requirement is monitored by the IG Team, which regularly reviews incidents reported on Datix to establish if they have been caused in whole or part by DPIAs not being appropriately completed. To ensure projects appropriate complete DPIAs, there will be IG membership / attendance / review of minutes at the Trust's various IM&T groups.

8.0 REFERENCE TO OTHER DOCUMENTATION

Other documents to be read in conjunction with this policy and its associated procedures are:

- General Data Protection Regulation 2016
- Data Protection Act 2018
- Data Privacy Impact Assessment Handbook – Information Commissioner Office
- Information Governance and Security Policy

END

APPENDIX 1

CONSENT FORM – FOR USE OF SMS TEXTING

Consent to receive appointment reminders by SMS text message

APPOINTMENT REMINDER BY TEXT (Example)

We will contact you approximately 2 weeks before your appointment due date.

The text will not identify the sender and will read as follows:
'Appointment reminder: Date and Time'

Please let us know if your phone is lost, stolen or you have changed your number

The health practitioner may wish to contact you by SMS Texting to remind you about a forthcoming appointment.

☐ I agree to the service communicating with me by Short Messaging Service (SMS or Text)

☐ I confirm that the mobile number the service holds on my record is correct and I will notify them of any changes.

☐ I agree to receive a reminder of my appointment by SMS

☐ I agree to receive a reminder of my daughter/son's appointment by SMS

☐ I am aware that I can withdraw consent at any time by informing the Health Professional either verbally or in writing.

NHS Number: …… DOB: ……
(To be completed by Health Professional)

Name of Service User ……... …….

Name of Parent/Carer ……..……..……...

(If parent/carer of a child under 16 years / a service user that does not the capacity to consent on their own)

Consent obtained by:

Name: …….. Speciality:……...

Signature: …… Date:……....

CPG50F - SMS TEXT MESSAGING TO SERVICE USERS PROCEDURE

APPENDIX 2

How to Request Enablement of SMS Text Messaging within SystmOne

SystmOne has the functionality to send text messages to service users to confirm appointments or cancellations and to send reminders, reducing the level of DNA's. The SystmOne Team can enable SMS Text Messaging at any time however, prior to initiation of each service, assurance must be obtained from the Service Lead that processes are in place, and that Trust policies are being followed in line with the current Information Governance and Trust SMS Text Messaging Procedure (which can be located via the Trust Intranet).

Once the set-up processes are in place, as detailed below, please complete and sign the following declaration, attach to a Change Request Form and send to the SystmOne Team via systmonesupport@nhs.net

Once the Change Request has been received, the SystmOne Team will action SMS Text Messaging and contact the Service Lead to confirm this has been enabled, providing all the necessary set-up guidance documents.

SET-UP PROCESS (to be completed by the Service Lead)

1. Service to contact the ITT Service Desk, requesting an NHS Mail Account, unique for the purpose of sending SMS Messages via SystmOne.

2. Once the NHS Mail account details are confirmed, Service to complete a Change Request Form, attaching the completed declaration of interest form, and send to the SystmOne Team via systmonesupport@nhs.net

3. Each service must also decide how consent will be obtained and evidenced within the patient record, this can either be:-

a.) A signed and scanned consent form (example attached) or
b.) Verbal consent gained, evidenced by transcript of conversation within the patients notes, confirming details of how SMS will be used (as per the consent form).

4. An internal process for each service must be in place to determine how SMS will be used.

SMS TEXT MESSAGING TO SERVICE USERS PROCEDURE

SYSTMONE SMS TEXT MESSAGING SERVICE

Declaration of Due Process

Prior to enablement of the SystmOne SMS Text Messaging service, each Service Lead is required to complete and return this form in conjunction with a Change Request and send to the SystmOne Team.
This can be done via the Internal Mail or scanned and emailed to systmonesupport@nhs.net

……
(Name and Title of Service Lead)

……

I am aware of the Trust SMS Text Messaging Procedure and whereabouts it is stored on the Intranet (and have communicated this to my Team)
I am aware of the Trust Information Governance Policy and whereabouts it is stored on the Intranet (and have communicated this to my Team)
I confirm the Service will obtain a consent form from the Service User or their parent / carer / guardian prior to sending text messages
I confirm the Service will obtain a verbal consent from the Service User or their parent / carer / guardian prior to sending text messages and record this within the patient record
I confirm the Service has processes in place for the safe storage of scanned consent forms.

Essex Partnership University
NHS Foundation Trust

SMS TEXT MESSAGING TO SERVICE USERS PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG50F
VERSION NUMBER	3
KEY CHANGES FROM PREVIOUS VERSION	Three year review; amendment under s6
AUTHOR	Information Governance Manager
CONSULTATION GROUPS	IGSSC
IMPLEMENTATION DATE	October 2017
AMENDMENT DATE(S)	September 2018; March 2022
LAST REVIEW DATE	March 2022
NEXT REVIEW DATE	March 2025
APPROVAL BY INFORMATION GOVERNANCE & SECURITY SUB-COMMITTEE	February 2022
RATIFICATION BY QUALITY COMMITTEE	March 2022
COPYRIGHT	

PROCEDURE SUMMARY

Staff working for EPUT will ensure that they comply with the requirements of the Data Protection Act and safeguard the confidentiality of any personal information which is held.

This procedure should be read in conjunction with the Trust's Information Governance & Security Policy, Information Sharing & Consent Policy and associated procedures.

The Trust monitors the implementation of and compliance with this procedure in the following ways:

These procedural guidelines will be monitored and reviewed in line with Trust policy every three years and / or in line with changes to national / local guidance.
Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

The Caldicott Network and Information Governance Steering Committee will oversee the implementation of these procedural guidelines

Services	Applicable	Comments
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SMS TEXT MESSAGING TO SERVICE USERS PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

SMS TEXT MESSAGING TO SERVICE USERS PROCEDURE

Assurance Statement

Staff working for EPUT will ensure that they comply with the requirements of the Data Protection Act and safeguard the confidentiality of any personal information which is held.

This procedure should be read in conjunction with the Trust's Information Governance & Security Policy, Information Sharing & Consent Policy and associated procedures.

1.0 INTRODUCTION

1.1 The Essex Partnership University NHS Foundation Trust (the "Trust") supports the use of Text Messaging (or SMS – Short Message Service) as a means of communication, **subject to compliance** with this procedure.

1.2 A 'user' in this procedure is an NHS employee or any other person working for or on behalf of Trust.

1.3 Although the basic principles of SMS have been available for a number of years, it is recognised that it is an ever-growing technology. Accordingly, this procedure will be reviewed annually and users should ensure they follow the most recent version of the procedure, which will be available on the Trust's Intranet

2.0 PURPOSE OF THE PROCEDURE

2.1 This procedure sets out the circumstances in which service users may be contacted by SMS / Text Messaging and the procedures that must be followed when using this method of communication.

2.2 Services must individually agree the need/benefit of using SMS and formally approve and document the implementation of the service. Individual users must not use SMS for health-related purposes without formal documented approval.

2.3 Local/departmental procedures for the use of SMS, which comply with this procedure, must be documented and cover the following topics:-

- Identification of the need or justification for the use of SMS
- Identification of the service or facility to be provided
- The agreement to the use of the service by its intended beneficiaries/recipients
- Clear identification of the associated risks and of the means by which these risks are managed

- Storage and retention procedures (in particular, service user messages or important Trust messages)

3.0 USE OF SMS

3.1 SMS can be used for a number of purposes:-

- To send individual clients/patients appointment reminders
- To broadcast messages to a wide-ranging audience, for example, as a health promotion exercise
- To support a lone worker
- Messages to Staff and Team Members to assist staff movements/shifts

3.2 Advantages of using SMS to communicate with service users are:-

- Quick and easy communication without delays
- Reduced postage costs
- Reduced possibility of communications going astray through incorrect postal addresses, changing addresses of service users etc.
- Ability to send appointment reminders to reduce DNAs

The above examples are not exhaustive.

4.0 KEY POINTS OF THE PROCEDURE

4.1 SMS or text messaging is an attractive technology for quick communication of short messages and is a widely accepted form of communication. Service users therefore increasingly expect the Trust to communicate with them in this way for simple transactions such as appointment reminders.

4.2 The Trust endorses the use of SMS to communicate with service users provided this is for simple communications such as appointment reminders and provided strict Trust protocol (outlined below) is followed when sending messages.

NHS.net mail accounts should be used when sending out appointments or reminders. This means that teams/services must either set up a generic (team account) or individual nhs.net email account prior to sending SMS messages to service users.

- A Trust approved system with a secure SMS service.
- A generic email account is one that refers to a service or function rather than an individual e.g. EPUTreminders@nhs.net
- Explicit informed consent should be gained from service users prior to any SMS messaging taking place.
- SMS messaging must not be used for confidential/sensitive person identifiable information such as test results or discharge summaries. It must be used only for appointments and other non-person identifiable information.

- Under NO circumstances whatsoever should any type of person identifiable patient or staff data is transmitted via SMS.

- The SMS message will form part of the patient record and therefore should be stored within the patient record, as appropriate

5.0 CONSENT

5.1 Where patients or members of the public are the intended recipients/beneficiaries of a health-related service, they must consent to this. Informed consent is gained from the service user prior to the commencement of SMS messaging taking place and potential benefits and risks should be explained before deciding on whether or not to participate.

5.2 This could be achieved at the time of recording a mobile phone number. Retrospectively, this must be done by making contact with the intended recipient before initiating the service for that person.

5.3 Consent should be recorded within the patients' record.

5.4 Where it is not possible to record the consent within a system, a consent form (Appendix 1 or appendix 2) must be signed and where possible, scanned into the record or stored securely onsite ensuring there is a file note relating to the patient's consent.

5.5 Service users may withdraw their consent to receive SMS messages at any time by informing their Health Professional.

5.6 If a service user does not have the capacity to consent to SMS messaging then the carer should be consulted as appropriate.

5.7 Disciplinary action may be taken if the procedure is not followed

6.0 UNDER 16'S

6.1 **Messages can be sent to children under the age of sixteen following an initial discussion with the child and parent informed by assessment of capacity.** Where it is not appropriate for text to be sent directly to children under sixteen years of age it will be taken that the mobile number given is that of a parent-guardian/carer and is acceptable to use if permission to text is given.

7.0 RISKS

7.1 The risks associate with this technology will vary according to the outcome the user is seeking to achieve.

7.2 A Data Privacy Impact Assessment (DPIA) should be completed prior to the implementation of the service.

7.3 In areas where it is felt that risks are unacceptable, the service must not be implemented.

7.4 The following risks must always be taken into account:

Confidentiality risks can be mitigated to a large extent by only sending non-person identifiable messages and by never sending sensitive data such as – 'your next ante-natal appointment is…'

With particular regard to patients/clients, this must be the primary concern of users.

The following points must be addressed:-

- Ensuring delivery to the correct recipient (i.e. the 'safe haven' principle; the parent/carer of a child under the age of sixteen; the sender must be sure that the phone number being used is that of the intended recipient – being aware that phones are regularly changed, exchanged or sold)

- Theft of the recipients phone

If a service wishes to contract with an external provider of SMS Test Messaging, it must seek approval from Information Governance and ensure all contractual and security measures are in place before any agreement takes place.

7.5 Contract details of the service user should be check at every appropriate contact to ensure the details are correct within the patient record.

8.0 EQUALITY IMPACT ASSESSMENT

Text messaging can undoubtedly be of benefit to recipients, for example, those with hearing impairment or those who would benefit from appointment reminders. However, this procedure cannot address every issue that may arise from the use of SMS and an Equality Impact Assessment has been completed.

9.0 AUDIT

Auditing procedures will be established by Information Governance, in collaboration with the Head of Performance to ensure;

- The service does not create problems or difficulties for the Trust or for service users.
- An Owner or Local Trust Administrator (LOA) of the NHSmail account should monitor activity, assess risks and audit the effectiveness of the service.
- Risks are identified, regularly re-assessed and adequately addressed
- The service is providing good value to the Trust and to users
- Confidentiality or the Human Rights of the service user are not put at risk

- The procedure will be reviewed at least annually or in line with Trust policies and procedures.

10.0 TRAINING

All staff are responsible for their own actions and must maintain an up to date awareness of legal and ethical issues concerning the subject.

11.0 MONITORING ARRANGEMENTS

11.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

11.2 Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

11.3 The Caldicott Network and Information Governance Steering Committee will oversee the implementation of these procedural guidelines

12.0 RELATED DOCUMENTS

12.1 **Trust Policies and Procedures**

12.1.1 Information Governance & Security Policy and associated Procedures
12.1.2 Data Protection & Confidentiality Policy and Procedure
12.1.3 Freedom of Information Policy and Procedure
12.1.4 Corporate Records Management Policy and associated Procedures
12.1.5 Records Management Policy and associated Procedures
12.1.6 Information Sharing & Consent Policy and Procedure
12.1.7 Mobile Phone Policy and associated Procedures
12.1.8 Other relevant policies and procedures not mentioned

12.2 **National Legal Statutes**

12.2.1 Data Protection Act 2018
12.2.2 Human Rights Act 2000
12.2.3 EU Privacy and Monitoring Directive 2000
12.2.4 Regulation of Investigatory Powers Act 2000
12.2.5 Freedom of Information Act 2000
12.2.6 Computer Misuse Act 1990 and amended 2006
12.2.7 Copyright, Design and Patents Act 1998
12.2.8 Caldicott 2
12.2.9 Sexual Offences Act 2003
12.2.10 Health & Social Care Act 2012
12.2.11 NHS Constitution
12.2.12 Records Management Code of Practice
12.2.13 NHS Information Governance – Short Message Service (SMS) & Texting Guidance
12.2.14 General Data Protection Regulation

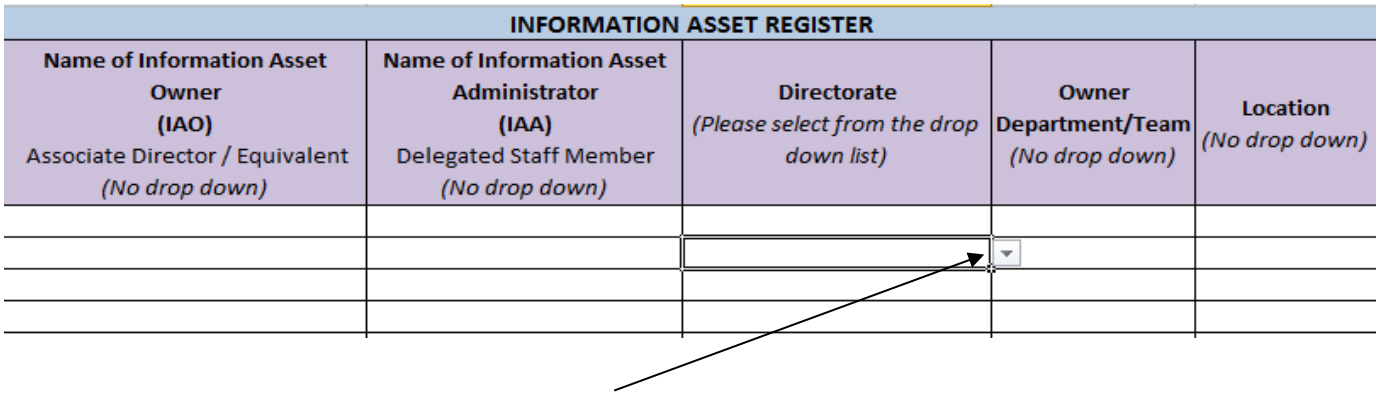
END

Essex Partnership University
NHS Foundation Trust

Guidance to the Information Asset Register spreadsheet. **Appendix 1 – CPG50g**

Further to the email, here is a step by step guide on how to complete the spreadsheet column by column.

How to choose form the drop down menu – if you click on the cell in which you would manually input your information, there will be a little arrow appear on the right hand side of the cell. Click on the arrow and the options shall appear…



INFORMATION ASSET REGISTER				
Name of Information Asset Owner (IAO) Associate Director / Equivalent *(No drop down)*	**Name of Information Asset Administrator (IAA)** Delegated Staff Member *(No drop down)*	**Directorate** *(Please select from the drop down list)*	**Owner Department/Team** *(No drop down)*	**Location** *(No drop down)*

Once you have clicked on the cell the dropdown will appear on the right hand side of the cell.

Column A: - **(IAO)** this will be the Associate director or equivalent

Column B: - **(IAA)** this is the name of the staff member completing the spreadsheet that has been delegated by the IAO

Column C: - **(Directorate)** Here if you click on the drop down box where an arrow shall be displayed on the right hand side, you can then choose from the list given as to what is relevant.

Column D: - **(Owner team/department)** this is the name of the IAO Department and team. Please select from drop down.

Column E: - **(Location)** this is the location of the team/department

Column F: - **(Type of master asset)** uses the drop down and chooses as appropriate.

Column G: - **(Name of asset)** this is the name of the asset e.g. IG incident files

Column H: - **(Details of asset)** this is a short description of what the asset is e.g. IG incidents reported by staff

Column I: - **(storage)** this is information where the asset is stored. Select appropriate drop down

Column J: - **(information asset contains)** Please select appropriate drop down

Column k: - **(Retention period)** Please select option from drop down

Column L: - **(usage)** how often is the asset used. Please select from drop down

Column M: - **(disposal method)** Please select option from drop down

Column N: - **(Criticality)** Protection against disruption

Column O: - **(Notes)** any additional notes

CPG50g - Appendix 2

EXAMPLE ASSETS Information Asset name or unique descriptor	**Location of the Asset or its components**	**Information Asset Type**
Assurance, Strategy and Planning		
Risk Register	Networked resource (Shared Drive)	Functional Management Information System
Business Continuity Planning	Networked resource (Shared Drive)	Functional Management Information System
Governing Body, Clinical Cabinet, People's Council, Audit Committee, Finance and Information Group Minutes and Papers	Networked resource (Shared Drive)	Functional Management Information System
Patient Experience		
PALS Database and related documents	Networked resource (Shared Drive)	Patient Information System
Complaints Database and related documents	Networked resource (Shared Drive)	Patient Information System
Quality and Patient Safety		
Serious Incidents Database	Networked resource (Shared Drive)	Other Information System
Health & Safety Database (RIDDOR)	Networked resource (Shared Drive)	Functional Management Information System
Safeguarding Databases	Networked resource (Shared Drive)	Other Information System
Contract Documents	Networked resource (Shared Drive)	Functional Management Information System

Internet/Intranet and email systems	Hosted System	Other information System

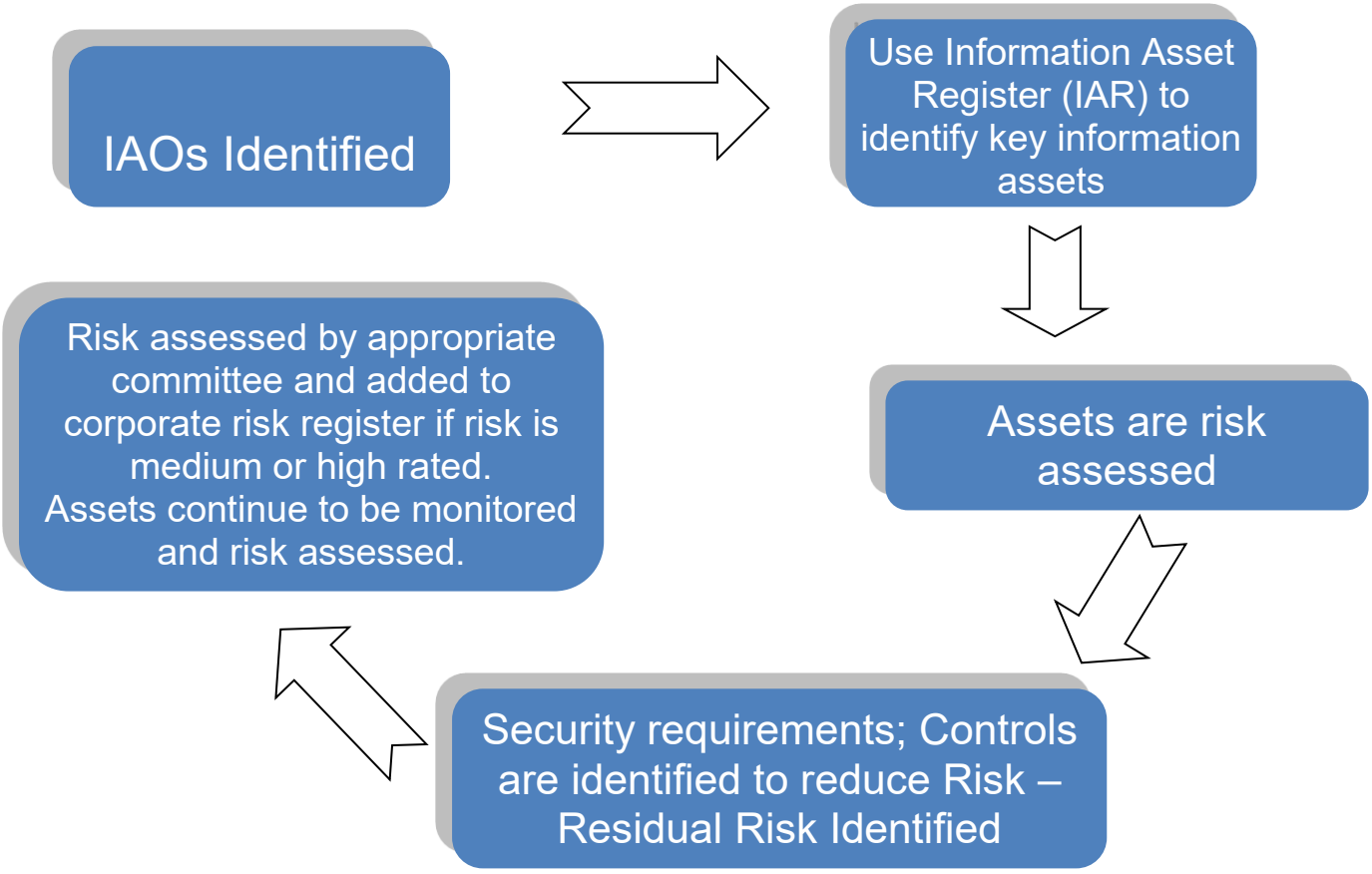
Other Asset Types	
People/staff	Human Resources
Hardware **Other Hardware (furniture)**	IT Provider Estates
Software	IT Provider
Personnel, health and Pension records	Human Resources
Company Financial Records	Finance

INFORMATION ASSET RISK ASSESSMENT PROCESS

Process

The information asset is risk assessed using the IAR on an annual basis (determined by the type of asset involved and whether there have been any major organisational changes). The risk report is reviewed by the Senior Information Risk Owner and any moderate or high risks assessed for reporting on the Trust corporate risk register. The risk assessment reminders are sent out to the IAOs to refresh and update on an annual basis and also for addition of any newly identified information assets.

Overview of Risk Assessment Process



Any new processes, systems or information assets that are introduced will be identified by the IAO in order to ensure that any impacts to information security, confidentiality or integrity are identified prior to implementation and initiation of any new system. Privacy Impact Assessments screening is performed if appropriate and these are reviewed and approved by the Information Governance or senior manager.

RISK ASSESSMENT MATRIX

Risk Priority

Key: Red – High Risk Amber – Medium Risk Green – Low Risk

RISK MATRIX					
5 – Very High	A	A/R	R	R	R
4 - High	A	A	A/R	R	R
3 - Medium	A/G	A	A	A/R	A/R
2 - Low	G	A/G	A/G	A	A
1 - Very low	G	G	G	G	G
Impact	**1 - Rare**	**2 - Unlikely**	**3 - Possible**	**4 - Likely**	**5 - Almost Certain**
	Likelihood				

Risk Matrix – Likelihood		
Likelihood rating		**Description**
5	Almost Certain	this type of event will happen frequently
4	Likely	this type of event will happen, but is not a persistent concern
3	Possible	this type of event may well happen (e.g. 50/50 chance)
2	Unlikely	unlikely that this type of event will happen
1	Rare	cannot believe that an event of this type will occur in the foreseeable future

Risk Matrix – Descriptor of Impact

	1	2	3	4	5
DESCRIPTOR	**INSIGNIFICANT**	**MINOR**	**MODERATE**	**MAJOR**	**CATASTROPHIC**
Injury	Minor injury not requiring first aid	Minor injury or illness, first aid treatment needed	Over three days off "sick" = **RIDDOR** reportable. 10 days to report to the HSE.	Major injuries, or long term incapacity / disability (loss of limb)	Death or major permanent incapacity
Patient Experience	Unsatisfactory patient experience not directly related to patient care	Unsatisfactory patient experience - readily resolvable	Mismanagement of patient care – short term effects	Mismanagement of patient care – long term effects	Totally unsatisfactory patient outcome or experience
Complaint/ Claim Potential	Locally resolved complaint	Justified complaint peripheral to clinical care	Justified complaint involving lack of appropriate care	Multiple justified complaints	Multiple claims or single major claim
Objectives/ Projects	Insignificant cost increase/schedule slippage. Barely noticeable reduction in scope or quality	< 5% over budget/schedule slippage. Minor reduction in quality/scope	5 -10% over budget/schedule slippage. Reduction in scope or quality requiring client approval	10 - 25% over budget/schedule slippage. Doesn't meet secondary objectives	> 25% over budget/schedule slippage. Doesn't meet primary objectives
Service/ Business Interruption	Loss/interruption > 1 hour	Loss/interruption > 8 hours	Loss/interruption > 1 day	Loss/interruption > 1 week	Permanent loss of service or facility
Human Resources/ Organisational Development	Short term low staffing level temporarily reduces service quality (< 1 day)	Ongoing low staffing level reduces service quality	Late delivery of key objective/service due to lack of staff (recruitment, retention or sickness). Minor error due to insufficient training. Ongoing unsafe staffing level	Uncertain delivery of key objective/ service due to lack of staff. Serious error due to insufficient training	Non-delivery of key objective/ service due to lack of staff. Loss of key staff. Very high turnover. Critical error due to insufficient training
Financial	Small loss (> £100)	Loss > £1,000	Loss > £10,000	Loss > £100,000	Loss > £1,000,000
Inspection/ Audit	Minor recommendations. Minor non-compliance with standards	Recommendations given. Non-compliance with standards	Reduced rating. Challenging recommendations. Non-compliance with core standards	Enforcement Action. Low rating. Critical report. Multiple challenging recommendations. Major non-compliance with core standards	Prosecution. Zero Rating. Severely critical report
Adverse Publicity/ Reputation	Rumours	Local Media - short term	Local Media - long term	National Media < 3 Days	National Media > 3 Days. MP Concern (Questions in House)

Essex Partnership University
NHS Foundation Trust

Information Asset Register Procedure

PROCEDURE REFERENCE NUMBER:	CPG50g
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	3 year review
AUTHOR:	Information Governance
IMPLEMENTATION DATE:	May 2018
LAST REVIEW DATE	May 2021
NEXT REVIEW DATE:	May 2024
APPROVAL BY IGSSC:	April 2021
APPROVAL BY QUALITY COMMITTEE	May 2021
COPYRIGHT	© 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
This document sets out the procedure to ensure that all information assets are identified and regularly assessed to ensure the confidentiality and security of the organisations information is maintained.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
All Information Governance Policies and the Information Governance Toolkit Developed in line with NHS England guidance and the Caldicott Review.

Services	Applicable	Comments
Trustwide	✓	IAO & IAA applicable

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

Information Asset Register Procedure

1.0 INTRODUCTION

1.1 This policy applies to Essex Partnership University NHS Foundation Trust, subsequently referred to in this document as 'the Trust'.

1.2 Information and information systems are important corporate assets and it is essential to take all the necessary steps to ensure they are protected at all times and are available and accurate to support the operation of the organisation. The Trust must ensure that all information assets that hold or process personal data are protected by technical and organisational measures appropriate to the nature of the asset and the sensitivity of the data. There should be formal information security risk assessment and management programme and operating systems under the organisations control must support appropriate access control functionality.

1.3 All information assets of the Trust should be identified and the Trust must have a nominated Senior Information Risk Owner (SIRO). The SIRO is required to ensure owners are identified for all Information Assets, Information Asset Owners (IAOs), with responsibility for managing the risks to those assets. Whilst responsibility for implementing and managing Information Asset controls may be delegated to Information Asset Administrators (IAAs) or equivalent, accountability should remain with the nominated owner of the asset.

1.4 The Department of Health has issued guidance to all NHS organisations on the process to be followed in identifying information assets, and allocating local ownership and responsibility for assessing any risk of data loss or information security for these assets. It is part of the guidance that risk assessments are performed regularly to ensure that the organisation complies with the Information Governance Assurance Programme and regular risk assessments are a requirement in the Information Governance Toolkit (IGT), which is mandated for all NHS organisations.

1.5 Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisations computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process personal confidential data (PCD) of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

2.0 OBJECTIVE

2.1 All information assets should be accounted for, understood, have a designated owner and be appropriately protected.
This will ensure compliance with:

- The Data Protection Act 2018 (DPA)
- The General Data Protection Regulation (GDPR)
- The Caldicott Report and subsequent review on personal confidential data
- The Information Security standard ISO 27001/2

3 SCOPE

3.1 The Information Asset Register Procedure applies to all business functions across the Trust, and covers information, information systems, networks, physical environment and relevant people who support those functions. It relates to both manual and electronic information, whether transmitted across networks or telephone lines, sent by fax, spoken in conversations or printed as hard copy (see **Appendix 2** for examples of information assets).

4 INFORMATION ASSET OWNERS (IAOs)

4.1 Information Asset Owners (IAO) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. The SIRO/IAO hierarchy identifies accountability and authority to effect change where required to mitigate identified risk

(see risk assessment process at **Appendix 3**).

4.2 The role of the Information Asset Owner is to understand what information is held, what is added and what is removed, how information is moved, who has access and why. As a result they should be able to understand and address risks to the information and to ensure that information is fully used within the law for the public good. The Information Asset Owner will also be responsible for providing or informing regular written reports to the SIRO, a minimum of annually on the assurance and usage of their asset.

4.3 The information asset owner will:

- ensure access to the asset is appropriately controlled in accordance with its classification and the Trust policies on information security, confidentiality, access and information sharing.

- ensure that the backup and business continuity arrangements are appropriate in accordance with its classification

- ensure that the asset is managed in accordance with the GDPR, DPA data protection principles and Caldicott Principles if the information asset processes Personal Confidential Data.

5 INFORMATION ASSETS

5.1 Information Assets (IA) are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation. Information assets are likely to include the computer systems and network hardware, software and supporting utilities and staff that are required to achieve processing of this data. Non-computerised records systems should also have an asset register containing relevant file identifications and storage locations.

5.2 Business processes and activities, applications and data should all be considered as Information Assets; however, their importance to the Trust may vary (Appendix 2).

6 INFORMATION ASSET REGISTER

6.1 Information Assets should be documented in a Trust asset register (IG Toolkit requirement, template at Appendix 1). In practice, a number of Trust asset registers may exist (e.g. departmental, HR Register, hardware register), and many will be *ad hoc*. As a priority, it is essential that all critical Information Assets are identified and included in this asset register, together with details of the 'Information Asset Owner' and risk reviews undertaken. The corporate Business Continuity Plan will also list these as critical information assets.

6.2 Each Information Asset Owner should be aware of what information is held and the nature and justification of information flows to and from the assets they are responsible for.

7 IDENTIFICATION OF NEW ASSETS

7.1 The Data Security & Protection Toolkit has a requirement for a documented plan to be developed to investigate and identify all remaining information assets that comprise or hold personal data and to assign responsibility for any identified, including details in the information asset register (IAR).

7.2 The Plan will be implemented by:

- Ensuring that Data Privacy Impact Assessments (DPIA) are included in any procurement process where new systems are implemented. This has a data mapping form within the template to ensure new assets are captured.

- The asset register will be reviewed by the Trust on a regular basis (at least annually) and circulated to all staff for them to review and refresh the asset register.

- The Asset Register will be reviewed at the Information Governance Steering Sub-Committee annually.

8 RISK

8.1 Appropriate security measures must be viewed as necessary for protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

The Threat — Of something damaging the confidentiality, integrity or availability of information held on systems or manual records.

The Impact — That such a threat would have if it occurred.

The Chance — Of such a threat occurring.

8.2 All new projects and procurements of IT systems will have a risk assessment as part of the project, and any existing systems should have periodic risk assessments, including those carried out by local management and internal/external audit services. Any risks identified as high must be reported to the Data Protection Officer (or equivalent) and if appropriate recorded on the IG risk register and/or escalated to the Trust corporate risk registers and Governing Bodies.

8.3 Controls can then be implemented to reduce the assessed risks in one of the following ways:

- Avoid the Risk
- Transfer the Risk
- Reduce the Threats
- Reduce the Vulnerabilities
- Reduce the Possible Impact
- Detect Unwanted events, react and recover from them.

There will always be residual risks and these should be reviewed on a regular basis to ensure that additional controls are having an effect on the likelihood rating. Risk Assessment Process is **Appendix 3.**

9 EQUALITY IMPACT ASSESSMENT

9.1 The Trust aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-

economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the Trust must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

10 DUE REGARD

10.1 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

11 PROCEDURE REVIEW

11.1 This procedure will be reviewed in line with Data Security & Protection Toolkit requirements or where changes occur in national policy or legislation.

END

Essex Partnership University
NHS Foundation Trust

NHSMAIL USAGE PROCEDURE

PROCEDURE REFERENCE NUMBER	CPG50H
VERSION NUMBER	3
KEY CHANGES FROM PREVIOUS VERSION	Appendices rescinded Various amendments and updates throughout
AUTHOR	Head of IT Infrastructure, Cyber & Assets & Deputy Data Protection Officer
CONSULTATION GROUPS	DSPT & Risk Working Group, Information Governance Steering Sub-Committee (IGSSC)
IMPLEMENTATION DATE	November 2018
AMENDMENT DATE(S)	Aug 2022; March 2023
LAST REVIEW DATE	March 2023
NEXT REVIEW DATE	March 2026
APPROVAL BY IGSSC	October 2022
RATIFICATION BY PORG	March 2023
COPYRIGHT	

PROCEDURE SUMMARY

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

The Trust monitors the implementation of and compliance with this procedure in the following ways:

Continual monitoring by IT Services

Services	Applicable	Comments
Trustwide	✓	

The Director responsible for monitoring and reviewing this procedure is Director of Information Technology and Telecommunication

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

NHSMAIL USAGE PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

NHSMAIL USAGE PROCEDURE

Assurance Statement

Staff working for EPUT will ensure that they comply with the requirements of the General Data Protection Act 2018 Regulation and safeguard the confidentiality of any personal information which is held.

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

1.0 INTRODUCTION

1.1 NHSmail is a secure national email service which enables the safe and secure exchange of sensitive personal/business and personal identifiable information for all email exchanges between other healthcare professionals using the nationally hosted NHS Mail service.

- ***"Personal Data"***
  Means any information relating 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

- ***"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.

1.2 NHSmail can be used to send sensitive/person identifiable information using the secure send feature ([Secure]) of NHS Mail to any other email system, details on how to do this are available in this document. This will automatically encrypt the contents of the email. You can also use the Egress system to send large amounts of information. The recipient will receive a secure link. Further information on this functionality can be found here - https://input.eput.nhs.uk/Staff/News/Pages/Egress-secure-communication.aspx

1.3 This document identifies EPUT's expectation for the use of NHS Mail.

1.4 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.

2.0 ACCESSING NHSMAIL

2.1 Staff can access NHSmail using:-

- A Trust issued device using Outlook
- The web-based interface (https://portal.nhs.net)
- Trust issued smartphone/tablet enabled with the trust mobile device management system (Airwatch)

2.2 Accessing email using non-Trust equipment at non-Trust location.

- Access NHSmail via the web based interface (https://portal.nhs.net). Do not use any other software to view this site.
- Select the default option of public or shared computer. The public computer option prevents you downloading information to a non-NHS device. You can view an attachment as a web page unless the document is password protected.
- Do not select private computer. Although you may be using your personal computer in your home, there is the potential for other members of your household to access or an external source with access to your networks.
- Staff must refer to records management guidance when exporting patient information from email.
- Remember the Trust's Code of Confidentiality - think about the sensitivity of what you view and who can see the screen.

2.3 You must not configure your personal mobile device to access NHSmail via any other means other than the web portal (https://portal.nhs.net)

- Some devices do not have built-in encryption at rest capability. Password/PIN does not guarantee a device has built-in encryption.
- Mobile devices keep a copy of emails on the device itself and the security of this data cannot be guaranteed and as a result is a breach of the trust IT security policy.

2.4 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;
- Phishing or spam emails

2.5 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.

2.6 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.

3.0 USE OF NHSMAIL

3.1 When sending emails be aware that:-

- When sending an email to a recipient for the first time, always select them from the Essex Partnership NHS Foundation Trust address book and not the global address list. (Recipients outside of NHSMail will not appear in the address book and will need to be entered manually, the first time) The chance of there being another person with the same name **is likely** within NHSmail and could result in confidential / sensitive information being sent to the wrong person. Wherever possible contact recipient by phone and confirm address for the first time.
- If sensitive information is received by the wrong recipient whether internal to the Trust or not, it is reportable via Datix as an information security incident and will be investigated.
- Do not include person identifiable information in the subject line of your email.
- Only include person identifiable information in the body of the email if you are confident that the recipient is entitled to see it and that the information can be shared with them.
- 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).
- 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.
- Delivery reports indicate that the e-mail has been successfully sent and will only be returned if the sender has requested it.
- 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.
- No e-mails may be sent externally outside of the Trust through the use of the automatic forwarding facility.

Important points to remember:-

- 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').
- 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.
- 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.
- 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.
- Emails can be disclosed to the public in response to a Freedom of Information, Subject Access or Environmental Information Regulations Request. Do not write anything in an email that could not be written in a letter or spoken face to face. Do not write anything defamatory about an individual or the organisation.
- Before sending your email, check: -
  - Your spelling (ensure you enable spell check if not already enabled)
  - The content is clear and correct;
  - The layout is consistent.
  - Do not assume that people read their email every day. Urgent messages are best communicated by phone in the first instance, and only sent by email as a backup.
  - Be selective - only send the email to those who really need it.

Important points to remember:-

- Information sharing agreements are published on the intranet in the Information Governance section. Information Sharing Agreements set out a legitimate reason for information to be shared with external organisations/third parties via email which staff within the trust are able to view.
- Consider who has access to the mailbox. Recipients may have assigned delegates who can read emails on their behalf.
- NHSmail is an encrypted service. You do not need to encrypt attachments when sending to another NHSmail mailbox. Emails will not be encrypted if they are forwarded onto another account which is not recognised as secure.
- If communication will be routine as part of an information sharing agreement, and the recipient does not have a secure email address, consider asking the ITT Service Desk to investigate creating a 3rd Party NHSmail account.

- Check the email address is accurate and secure before you send person identifiable information.
- Personal email accounts **must not** be used for work purposes.

3.4 **Distribution lists**

- ***Important points to remember:-***

  - Set the default address book to EPUT (https://input.eput.nhs.uk/Help/mail/User Guides Help Tools/Setting Outlook default Address Book.docx), this will allow internal staff to be easily found.
  - Distribution lists enable you to send one email to many people without needing to select each individual.
  - Staff who have left the Trust may continue to use their NHS mail address. Owners of distribution lists should review your distribution lists regularly to ensure that members who have left the Trust do not continue to receive Trust data.
  - Use distribution lists with care so that information is only communicated to those people with a need to know.
  - Global communication (All Staff) should only be sent by the trust Comms department.
  - There must be a business need for non-Trust individuals to be included in your distribution list.
  - Distribution lists are the responsibility of the owner and therefore it is the owner's responsibility to add/remove members.
  - For large groups of recipients always use the **"BCC"** option and not the "To" or "CC" options. This will protect email addresses and avoid the mistake of using "reply all".

3.5 **Receiving emails**

- ***Important points to remember:-***

  - Process or action your emails as soon as possible.
  - Set a reminder to yourself by marking items "urgent" or "flagged" for follow up.
  - Do not print emails unless absolutely necessary.
  - Once you have actioned an email, either delete or file it. See **Mailbox Management**.
  - Keep the number of emails in your Inbox to a minimum.
  - Make sure deleted items really are deleted by emptying the Deleted Items folder.
  - Manage any attachments you receive by either:
    - Filing the whole email (including attachments) in your email file system.
    - Saving either the whole email or the attachment separately on the network.

3.6 **Replying and forwarding emails**

- ***Important points to remember:-***

  - Only reply to or forward emails when necessary.
  - Be careful when using the "Reply to all" facility – consider who will see your reply.
  - Attachments are automatically removed when you use "Reply" and included when you use "Forward".

3.7 **Using the calendar**

- ***Important points to remember:-***

  - Staff who have left the Trust may continue to use their NHS mail address. Review access to your calendar regularly to ensure that it is restricted to Trust staff.
  - Meeting recipients leaving the Trust must be removed as an attendee by the meeting owner as soon as possible.
  - Your calendar must not contain any patient or personal identifiable information unless authorised by the Information Governance Team to ensure person/patient confidentiality is maintained.
  - Documents embedded in your calendar are viewable by all staff with the appropriate level of access to your calendar.
  - Hyperlinks to internal sites will not work if using NHSmail via a non-Trust network (e.g. EPROC approval emails).

4.0 MAILBOX MANAGEMENT

4.1 All emails generated in the course of NHS activity are Public Records. They are subject to the same legislation and operational requirements of any other Public Record. It is your responsibility to manage your email messages appropriately

The Trust endorses the use of SMS to communicate with service users provided this is for simple communications such as appointment reminders and provided strict Trust protocol (outlined below) is followed when sending messages.

4.2 Attachments – sending and saving **Important points to remember:-**

- NHS mail is provided for the secure exchange of information and not for long term information storage.
- **Review** your inbox and sent items regularly.
- **Save** attachments that you need to keep on your **shared drive**.
- **Save** corporate records on the network (shared drive) following Corporate Records Management Guidance.
- **Save** patient related information in the patients' record as per the Records Management Guidance.
- **Send a hyperlink** instead of an attachment if the recipient has access to the location where the document is saved.

- If sending an attachment that is saved on your shared drive, **remove** the attachment from your email in the **sent items** folder. Otherwise you are doubling the space needed to store any document you have created and emailed

4.3 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.

4.4 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.

4.3 **Mailbox limits**

- ***Important points to remember:-***

  - Your mailbox has a standard maximum size limit of 4 GB (see Appendix 1 – NHS mailbox quotas).
  - **All** email sub-folders **and** calendar items count towards the amount of space used in your mailbox - not just the mail in your Inbox. Look at the folders that are taking up the most space and decide whether you really need to keep all the messages in them. (I.e. you can see your mailbox usage by clicking on "file" option within Outlook.)
  - The maximum size of attachments is 27MB.
  - You will receive a warning when your mailbox is nearing its size limit.
  - If your mailbox reaches its size limit, you will be unable to send and receive email until you have removed a sufficient number of messages from your mailbox. You are responsible for ensuring that your mailbox is able to send and receive information.
  - If your mailbox is dormant for a period of time (30 days) then your account will be closed, and you will need to log back into your account to reactivate it.
  - Emails in your account may be deleted by the NHSmail system after 4 months of account inactivity. This is not controlled by the Trust therefore filing emails is important to ensure Trust information is not lost.
  - It is worth noting that the newly implemented Mailsafe system is now the Trust's email archive tool that will archive email over 90 days old and will assist in managing the user's mailbox size.
  - In exceptional circumstances, mailbox size limits can be extended but this should only be considered if the user's mailbox exceeds the standard 4 GB due to the user being responsible for large mail volumes/attachments that will regularly cause 3 months' worth of email to reach the limit. This option should not be used as a substitute for mailbox management and housekeeping.
  - To request an increase in mailbox size, the following criteria must be met:
    - Justification for why standard mailbox management has been unsuccessful
    - Explanation of the role of the user that constitutes an above average volume of mail/attachments.

  - Written approval by the Executive Director to support the above claims sent in via the Service desk self-service portal
- Mailbox extensions can only be undertaken by a member of the trust IT Department and only on the authorisation from a senior IT manager. A check will be made to identify if the mailbox limit has been reached or is 95% full (under 200mb of the 4 GB limit) and that all other attempts to reduce the size of the mailbox have been exhausted.

4.4 Shared mailboxes

- Shared mailboxes have an owner nominated to them who is responsible for managing that mailbox and allocating delegated access where necessary.

4.5 Deleting unwanted emails

- Deleting an email from your “Inbox” or “Sent Items” will move it to the “Deleted Items”. The email will not be permanently deleted until you delete it from “Deleted Items”, or you have set your “Deleted Items” to empty automatically.

5.0 ACCOUNT MANAGEMENT

5.1 New accounts

- New accounts are requested through the IT Self Service Portal (https://servicedesk.eput.nhs.uk/RSDPortal/Workflow/WorkflowHomepage) once approved by your line manager.
- You must accept the NHSmail Acceptable Use Policy upon first login to the NHS Mail platform and abide by all the statements in the policy - https://portal.nhs.net/Home/AcceptablePolicy
- All staff must set up their security questions and answers via the https://portal.nhs.net portal when setting up their NHSmail account. The questions and answers will be used in the event of the mailbox password being forgotten. The security questions and answers can be set up or changed at any point via the NHSmail portal.
- The IT Service Desk can reset passwords, but this will only be done if the user has already tried to reset/change their password themselves via the self-service NHSmail portal option.
- A mobile phone number must be provided in support of the secret questions for this function to work, if this is a personal mobile, it can be hidden from the address book.

5.2 Transferring an account from a different organisation

- You can transfer an existing NHSmail account from a different organisation. You must ask your previous organisation to mark you as a “leaver”. Only when this has been completed can the ITT service desk mark you as a “joiner” to the EPUT directory.
- You must ensure that your NHSmail account is cleared of all Trust related emails before your last day with EPUT. Managers and staff must work together to confirm this has taken place.
- Accounts may not be transferred if they relate to national enquires and these will be treated on a case by case basis.

5.3 **Closed accounts**

- Your line manager must follow the leavers' process and inform the ITT service desk when a staff member leaves the organisation. You **must** clear your mailbox of all Trust information prior to transferring to a new NHS organisation.

5.4 **Passwords**

- ***Important points to remember:-***

  - Your NHSmail account must have a unique password which you **must not share**; the password must adhere to the NHS mail Password Policy.
  - If you forget your password, you can reset the password yourself - staff are encouraged to attempt a password self-service reset through nhs.net portal prior to engaging any other support request.
  - If a self-service password reset is unsuccessful, please log your request via the EPUT IT Service desk at https://servicedesk.eput.nhs.uk
  - If it is imperative that your account is unlocked immediately, please contact 0300 123 5366 and hold for an agent to assist you.
  - You will be prompted to change your password every 90 days.

6.0 MONITORING OF EMAILS

6.1 The Trust retains the right to access an employee's email messages if it has reasonable grounds to do so. The contents of email will not be accessed or disclosed other than for security purposes, as part of an investigation, clinical safety when staff are on long-term sick, suspension etc. or as required by law, by application of the appropriate legal statutes.

6.2 Extended monitoring of individual mailboxes will only occur when there is a legitimate requirement to do so and only for as long as required; for example, where there is evidence or suspicion of email misuse.

6.3 All email will be automatically scanned for viruses, inappropriate content and unauthorised attachments by the NHSMail platform provider.

6.4 The Trust will work with NHSmail to find a reasonable process to ensure emails can be accessed appropriately and within a reasonable time period. The time period will be set by NHSmail as the system is managed by NHS Digital and the Trust has no control over this process

6.5 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

6.6 Where staff inadvertently access e-mail which may fall into the group above (6.5) this should be reported to the Trust's IT Service Desk (immediately.

6.7 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 is **not acceptable**
- 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.

6.8 Where staff are absent due to unexpected leave and access to the mailbox is required for operational reasons. The user's line manager should raise a ticket with the IT Service Desk who will then provide the relevant access.

6.9 Access to a staff member's mailbox without expressed consent can only be authorised by the Caldicott Guardian or delegated senior responsible officer.

7.0 MONITORING ARRANGEMENTS

7.1 These procedural guidelines will be monitored and reviewed in line with Trust policy, every three years and / or in line with changes to national / local guidance.

7.2 Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

7.3 The Caldicott Network and Information Governance Steering Committee will have overall responsibility for overseeing the implementation of these procedural guidelines.

8.0 RELATED DOCUMENTS

8.1 Trust Policies and Procedures

- Information Governance & Security Policy and associated Procedures
- Data Protection & Confidentiality Policy and Procedure
- Freedom of Information Policy and Procedure
- Corporate Records Management Policy and associated Procedures
- Records Management Policy and associated Procedures
- Information Sharing & Consent Policy and Procedure
- Mobile Phone Policy and associated Procedures
- Other relevant policies and procedures not mentioned
- NHS Mail usage policy

8.2 National Legal Statutes

- General Data Protection Regulation
- Human Rights Act 2000
- EU Privacy and Monitoring Directive 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Computer Misuse Act 1990 and amended 2006
- Copyright, Design and Patents Act 1998
- Caldicott 2
- Sexual Offences Act 2003
- Health & Social Care Act 2012
- NHS Constitution
- Records Management Code of Practice
- Data Protection Act 2018

END

PLEASE NOTE – THE PROCEDURE CODE CPG50I IS NOT IN USE.

Essex Partnership University

NHS Foundation Trust

EPUT Cyber Incident Response Procedure

PROCEDURE REFERENCE NUMBER:	CPG50K
VERSION NUMBER:	2
KEY CHANGES FROM PREVIOUS VERSION	-Additional wording added to s1 – Incident Response Team -Additional wording added to s4 "Playbook instructions to include…" -Updates to titles for 'Incident Response Team' -Update to the monetary values in the Severity Matrix
AUTHOR:	Deputy Data Protection Officer
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE:	April 2022
AMENDMENT DATE(S):	N/A
LAST REVIEW DATE:	May 2023
NEXT REVIEW DATE:	May 2026
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	April 2023
RATIFICATION POLICY OVERSIGHT & RATIFICATION GROUP:	May 2023
COPYRIGHT	

PROCEDURE SUMMARY
These procedural guidelines will ensure that the strategic risk associated with not having a procedural document in relation to a cyber-attack will minimise the impact and effect recovery of service, in a co-ordinated approach within and throughout the Trust.
The Trust monitors the implementation of and compliance with this procedure in the following ways:
The Information Governance Steering Sub Committee and Quality Committee will have overall responsibility for overseeing the implementation of this procedure and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust. The Cyber Security Team and Information Governance Steering Sub-Committee will be responsible for overseeing the operational implementation of this procedure and its associated procedures, as appropriate

Services	Applicable	Comments
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CYBER INCIDENT RESPONSE PROCEDURE

CONTENTS

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

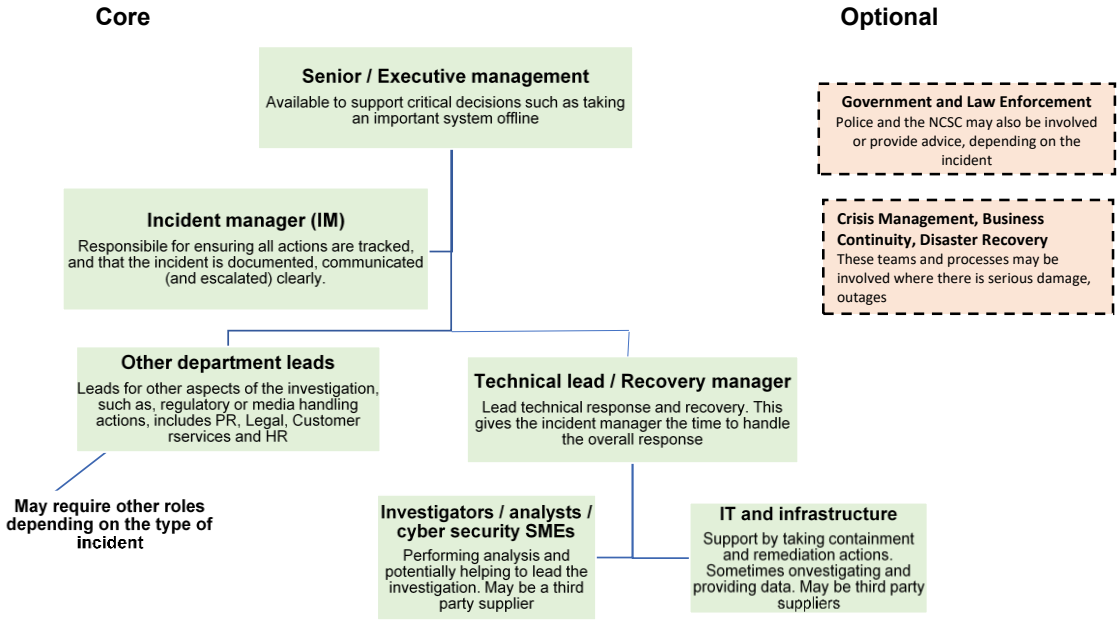
CYBER INCIDENT RESPONSE PROCEDURE

1. INCIDENT RESPONSE TEAM

A cyber security incident response team (CSIRT) consists of the people who will handle the response to an incident. It may include both internal and external teams and may differ based on the nature of the incident. The Early Preparedness and Resilience Team may be notified by NHSX and NHS Digital from the cyber resilience team to enact incident response.

The diagram below details the core roles which will be needed during an incident. Some individuals may perform more than one role, but the responsibilities must be accounted and available as needed, if an incident is to be handled smoothly.

Optional roles are listed, pulling in external teams and additional business management functions.



Incident Response Team:

- NHS England and/or other authority
- Trust Business Continuity and Disaster Recovery Representative
- Information Technology (IT)
  - Deputy Director of Digital and Business Intelligence (Deputy CIO)Interim Associate Director for IT Business Operations
  - Associate Director for IT Technical Strategy and Projects/Information Security Manager
  - Associate Director for Digital Service Development
  - Associate Director for Business Analysis and Reporting
- Senior Management
  - Director of ITT, Business Analysis & Reporting (CIO)Executive Director of Strategy, Transformation and Digital (Senior Information Risk Officer)
- Legal Services
  - Director of Legal Services
- Communications
  - Director of Communications

- Human Resources (HR)
    - Chief Human Resource Officer
    - Executive Chief Operating Officer
- Insurance
    - Director of Risk and Assurance

Ad-hoc contacts based on system or incident type, may be delegated from those staff above

- Head of Service or appropriate management to make operational decisions
- Contacts to carry out the tasks to fix or reduce the impact of the incident

Always consider the risk of people being unavailable - ideally include at least 2 contact methods and 2 or more people (or group) details.

Out of hours cover needs to be considered when identifying each role to cover the incident in hours and out of hours.

The Major Incident Manager will set up the conferencing method and inform the Incident Response Team through Teams, email and/or text.

2. ESCALATION CRITERIA

Typically, matrices are used to determine the severity or priority of an incident. The severity level will inform how quickly the incident needs to be handled and who it might need to be escalated to.

For example, a high or critical severity incident is likely to always need to go up to CEO or board level. A low priority incident could most likely be handled by the IT security team alone. You should document who the escalation points of contact are, along with their contact details (including out of hours) and how quickly the escalation needs to occur.

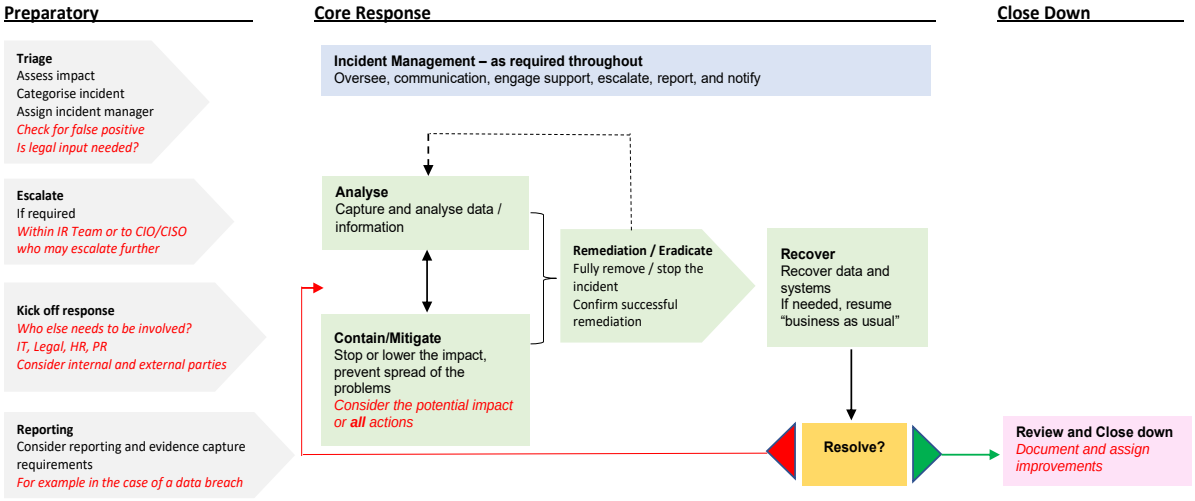
The people escalated to must have the authority to make critical decisions. For example, when a decision may result in major business impact, such as taking a critical service or system offline.

Identify the people who are empowered (or who hold delegated authority) to make such decisions and ensure the escalation process includes these key personnel, as appropriate. It is also important to consider deputies and a process to enable others to make decisions, should the primary contact not be available.

In addition to generic guidance, it may be useful to identify specific situations where the technical team should act autonomously, based on the highest business risks and where taking early containment action is likely to reduce the impact of particular incidents.

3. INCIDENT RESPONSE PROCESS

The diagram below provides an example of a high-level incident response process, with guidance notes in red.



Incident management - communications, overseeing, tracking, and documenting

Incident management collects together the co-ordinating functions which guide, inform, and support the whole response process. It encompasses a number of aspects, including:

- Tracking, documenting, assigning, and correlating all findings, tasks and communications. (*Note that keeping careful track of the whole response is very important in cases which may later be reviewed by regulators or courts. This includes real or potential data breaches and criminal activity.)*
- Arranging of regular update meetings or calls, and involvement of relevant teams
- Escalating serious incidents to senior management
- Ensuring the incident is communicated appropriately (to team, wider business, other stakeholders)
- Ensuring that the full incident lifecycle is covered from initial discovery through to close down.

Consider options for secure or alternative communications in event of a sensitive incident, or where normal channels are unavailable due to network/email/phone system outage.

Clarity is critical

Understanding everyone's roles and responsibilities is central to ensuring an incident is managed, and therefore handled, successfully.

There must be a central point of co-ordination, no matter who is involved, to ensure all findings are correlated and actions are planned.

Keeping a careful record of the incident response, decisions made, actions taken, data captured (or missing) is incredibly useful for post-incident reviews. This is especially true if you will need to present evidence of your response to a regulatory body.

Triage - understanding the type and severity of an incident

Understanding the type and severity of an incident allows you to determine how urgent your response is. It also enables you ensure that the correct people are involved from the outset.

There are two aspects to look at when assessing an incident: **Severity** and **category**, or type.

Severity is typically considered against the following:

1. **Availability** – is the availability of data or systems impacted? (I.e. what is the impact on business output?)
2. **Confidentiality** – has sensitive data been accessed, leaked or stolen?
3. **Integrity –** could data or systems have been altered such that they cannot be trusted?

With all of the above, consideration should be given to the scale of the problem, to what type of system or data is involved, and the practical consequences of the incident.

When quantifying impact, it can help to have full documentation detailing all critical assets and data.

Severity matrix

To aid the evaluation of incident severity, create a matrix of example outcomes, rated for severity. These will help inform how serious the response to the incident should be, who needs to be involved and whether the response needs to take priority over other activities.

Below is an example severity matrix. We should think carefully about what matters most to your business and tailor the Examples column to fit your organisation:

Severity	Examples
Critical	• Over 80% of staff (or several critical staff/teams) unable to work • Critical systems offline with no known resolution • High risk to / definite breach of sensitive client or personal data • Financial impact of £6,500,001 • Severe reputational damage - likely to impact business long term
High	• 50% of staff unable to work • Risk of breach of personal or sensitive data • Noncritical systems affected, or critical systems affected with known (quick) resolution • Financial impact of £ 2,500,001 - £6,500,000 • Potential serious reputational damage
Medium	• 20% of staff unable to work • Possible breach of small amounts of non-sensitive data • Low risk to reputation • Small number of non-critical systems affected with known resolutions
Low	• Minimal, if any, impact • One or two non-sensitive / non-critical machines affected • <10% of non-critical staff affected temporarily (short term)

Categorisation of an incident

The Incident Response Team need to determine what type of incident the Trust is facing.

Some examples include:

- **Malicious code:** Malware infection on the network, including ransomware
- **Denial of Service:** Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- **Phishing:** Emails attempting to convince someone to trust a link/attachment.
- **Unauthorised Access:** Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.
- **Insider:** Malicious or accidental action by an employee causing a security incident.
- **Data breach:** Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- **Targeted attack:** An attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories).

Category matrix

As with severity, it is very useful to create a matrix of the different categories.
You can enhance this by adding examples of different severity incidents alongside each category. This will help guide and inform your response.

Response stages

The descriptions below provide information for each of the four core response stages of an incident response cycle.

- **Analyse**

  This stage of the incident involves everything from technical analysis through to a review of social media reactions.

  It is important to ensure tasks are prioritised carefully and findings are constantly reviewed and correlated, as these may lead to new tasks.

  Usually, the initial priority is to understand enough to take containment/mitigation actions and ultimately remediate the attack.

- **Contain / Mitigate**

  Once you're certain it's safe to do so, you should take steps to reduce the impact of the incident and prevent things from getting worse. This usually involves such things as blocking activity, isolating systems and resetting accounts. It may also involve non-technical actions such as media handling.

  This stage may require critical decisions such as taking a core business system offline. It is important to consider the consequences of any such actions, both good and bad. You should also evaluate the possibility that the attacker might react to your actions, or bury themselves more deeply in the network (often in the case of targeted attacks). In some cases, it may be better to monitor and analyse further before action is taken.

- **Remediate / Eradicate**

  The aim of this stage is to fully remove the threat from your network and systems. This often involves similar actions to containment but is sometimes coordinated so that all actions are carried out simultaneously.

It is important to confirm that remediation has been successful before to moving to the recover stage - this may involve monitoring for a period. Some analysis may continue in this stage too.

- **Recover**

  At this point, systems are returned to 'business as usual'. Clean systems and data are put back online and, in some cases, final actions are taken to handle regulatory, legal, or PR issues.

Throughout the response, all tasks and findings should be tracked. Findings and analyses should be correlated, response actions re-prioritised.

In some cases, the response will need to be escalated or de-escalated.

Post incident review and close down - learning from the incident

A post incident review should cover:

- Lessons from the incident itself
  - Are there security improvements which could have prevented the incident, or enabled earlier detection?
  - Consider both the tactical fixes that would have prevented or detected this incident as well as strategic solutions that may only be identifiable across multiple incidents. For example, ineffective governance processes leading to multiple intrusions through previously un-recorded, internet-facing, assets.
  - In particular, was there any information which would have significantly helped your response, but which was difficult or impossible to obtain? Plan to gather this data ahead of any future attacks.

- Lessons from the response
  - Was the response successful and effective?
  - Were there elements which could have been handled better?
  - Was there data which could have been useful but wasn't available (For example, the right logs, or something that was overwritten early in the response?). Keeping a record of activities during the response will assist with this review.

4. PLAYBOOKS / GUIDANCE ON SPECIFIC TYPES OF INCIDENTS

A playbook (or runbook) is a detailed response plan, usually focused on a specific incident type.

Typical playbook examples include 'malware infection', 'phishing emails', ‘data breach' and so on.

It is recommended that we start with the top 3-5 most likely and high-risk incident types for a health organisation. To determine what these are, review previous incidents affecting your organisation as well as drawing on threat intelligence and general cyber security news, relevant to our sector and the countries in which we operate.

We should also consider those threats which apply globally, such as major ransomware attacks.

As a minimum, we should document a set of simple instructions which will cover at least the first few hours of each incident, as these can be the most critical and time pressured.

Playbook instructions should include:

- Who to contact – NHS England, CQC, Business BCP team, technical teams, suppliers, senior management, and when to engage Legal, HR, PR, if required?
- How to understand / triage the incident (specifics relating to this type of incident)
- Guidance on reducing the impact / preventing further impact - specific types of containment or mitigation actions
- Steps on retaining evidence or data if required

Enhanced playbooks

Further incident types and additional stages of guidance can also be included. For example, guidance on analysis, how to fully remediate and recover from the incident, how and when to close down, and how to perform a post incident review.

You should consider legal, media and regulatory aspects. Alternatively, the IR team's playbooks could just include guidance on when to engage these teams, who may have their own detailed guidance in this area.

Playbooks can also be implemented and embedded within incident management and orchestration systems, if appropriate.

5. LEGAL AND REGULATORY REQUIREMENTS

No matter the type of business, assuming the organisation is based in, or does business within the UK or EU, GDPR and DPA regulations will need to be adhered to.

Nearly all organisations will hold personal data for employees and for their customers. There may also be specific regulatory requirements for the sector, and potentially, specific customer reporting requirements based on any contractual agreements.

Minimum preparations in this area should include engaging legal advice and documenting:

- What constitutes a reportable incident, based on the types and volumes of data your business holds (including any data held by suppliers)
- When and how to engage legal support
- Extra steps required. For example, preservation of evidence or recording of actions taken

To further improve this, the following should also be considered:

- Create forms ready for any regulatory reporting
- Run workshops focused on scenarios which invoke legal / regulatory requirements and rehearse the appropriate steps

Law enforcement and evidential handling

If the decision is made to undertake any legal proceedings (e.g. prosecute a criminal) then there will also be a requirement to engage relevant law enforcement agencies. This (along with any civil cases) may require careful handling of evidence. Association of Chief Police Officers (ACPO) has advice on this process.

END