# RECORDS MANAGEMENT POLICY

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER</th>
<th>CP9</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER</td>
<td>2</td>
</tr>
<tr>
<td>REPLACES SEPT DOCUMENT</td>
<td>N/A</td>
</tr>
<tr>
<td>REPLACES NEP DOCUMENT</td>
<td>N/A</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td>Incorporated new General Data Protection Regulations</td>
</tr>
<tr>
<td></td>
<td>Reference made to Health Information Exchange</td>
</tr>
<tr>
<td></td>
<td>Removed all reference to Transportation of records – signposted to Transfer Transportation of Records procedure CP9f</td>
</tr>
<tr>
<td>AUTHORITY</td>
<td>Records Manager</td>
</tr>
<tr>
<td>CONSULTATION</td>
<td>Information Governance Steering Committee</td>
</tr>
<tr>
<td></td>
<td>Quality Committee</td>
</tr>
<tr>
<td></td>
<td>Paris Project Board</td>
</tr>
<tr>
<td></td>
<td>Mobius Project Board</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE</td>
<td>August 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S)</td>
<td>August 2018</td>
</tr>
<tr>
<td>LAST REVIEW DATE</td>
<td>August 2018</td>
</tr>
<tr>
<td>NEXT REVIEW DATE</td>
<td>August 2021</td>
</tr>
<tr>
<td>APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE</td>
<td>24th September 2018</td>
</tr>
<tr>
<td>RATIFIED BY QUALITY COMMITTEE</td>
<td>12th October 2018</td>
</tr>
<tr>
<td>COPYRIGHT</td>
<td>© EPUT 2018</td>
</tr>
<tr>
<td></td>
<td>All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner</td>
</tr>
</tbody>
</table>

## OPERATIONAL POLICY SUMMARY

The purpose of this policy is to set out the overall aims and objectives of the Trust in the effective management of its records. Effective records management is one element of information governance. There are records management standards in the Information Governance Toolkit and the achievement of Toolkit standards forms part of the overall Care Quality Commission assessment for the Trust.

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

- Monitoring of the availability of Clinical Records will be undertaken by the Trust’s Records Manager on a monthly basis. Should more than 4% be missing this will be reported to the Information Governance Steering Committee in the format of a report for action to be agreed.
- A three yearly audit will be undertaken by the Information Governance Department Process for retaining and disposing of records has been followed.
The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer.

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

RECORDS MANAGEMENT POLICY

CONTENTS

1.0 INTRODUCTION
2.0 DUTIES
3.0 DEFINITIONS
4.0 PRINCIPLES
5.0 RECORDS PROCEDURES
   5.1 Records Management Lifecycle
   5.2 Records Creation
   5.3 Records Storage
   5.4 Record Management/keeping
   5.5 Record Creation/Registration/Architecture
   5.6 Accessing Records/Security/Confidentiality
   5.7 Electronic Record Systems
   5.8 Retention and Destruction
   5.9 Storage
   5.10 Sharing and Disclosing Information
5.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE
6.0 POLICY REFERENCES/ASSOCIATED DOCUMENTATION
7.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES
This policy aims to ensure that the Trust has a systematic and planned approach to the management of records, from the moment they are created to their ultimate disposal which ensures that the organisation can control both the quality and quantity of the information that it generates; can maintain that information in a manner that effectively serves its needs, those of government, the law and of the citizen; and can dispose of the information efficiently when it is no longer required.

The principles of this policy apply equally to all records whether created paper, electronically or digitally, and includes both medical and corporate records, as the concern is the records content or information and not the medium of delivery.

1.0 INTRODUCTION

1.1 The purpose of this policy is to set out the overall aims and objectives of the Trust in the effective management of its records.

1.2 Effective records management is one element of information governance. There are records management standards in the Information Governance Toolkit and the achievement of Toolkit standards forms part of the overall Care Quality Commission assessment for the Trust.

1.3 The adoption of corporate procedures, practices and standards is essential to ensure effective records management is consistently applied throughout the Trust in a systematic and sustainable manner.

1.4 Recent legislation, particularly the Freedom of Information Act 2000, has a significant effect on records management in public authorities. The Trust must ensure that records management policies and procedures are fully compliant with the new legislation and with Government policy on the management of information.

1.5 In line with Information Governance Alliance Guidance 2016, The National Archives’ Records Management Standards and Guidance, the policy statement for the Trust is that it is committed to adopting:
1.6 The new data protection legislation came into effect in May 2018. The General Data Protection Regulation (GDPR) replaces the Data Protection Act 1998. Many of the main concepts and principles are much the same as those in the Data Protection Act 1998. The following regulations have been introduced –

The right to rectification -

This gives individuals the right to have incorrect personal data rectified or completed if incomplete.

The right to erasure -

This gives individuals the right to have personal data erased. The right to erasure is also known as ‘the right to be forgotten’.

The right to restrict processing -

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

The right to data portability -

This will allow a requester to ask for a copy of personal data in an electronical format.

The right to object -

This gives individuals the right to object to the processing of their personal data in certain circumstances

The Trust has one calendar month to respond to all of these requests.
2.0 DUTIES

2.1 The Information Governance Steering Committee (IGSC) is responsible for approving the content of this policy and monitoring its compliance and effectiveness.

2.2 The Quality Committee is responsible for noting the approval of this policy.

2.3 The Chief Executive with delegated responsibility to the Director of ITT and Senior Managers (defined as Band 8 or above) – are personally accountable for records management within the organisation. The following Directors have specific responsibility for ensuring compliance and that adequate procedures and good practice are in place within there are of responsibility

   (a) Clinical/health records (Executive Medical Director/Director of ITT)

   (b) Personnel and Administrative records (Executive Director of Corporate Governance)

   (c) Commercial/business records (Executive Chief Finance Officer / Deputy Chief Executive)

2.4 The Chief Executive has delegated responsibility for Caldicott issues to the Executive Medical Director, who has responsibility for reflecting patients’ interests regarding the use of patient identifiable information, together with ensuring that patient identifiable information is shared in an appropriate and secure manner.

2.5 The Data Protection Officer is responsible for the development, implementation, compliance, monitoring and review of the data protection legislation, including providing guidance on records management issues, and ensuring that related policies and procedures conform to the latest legislation and NHS guides on data protection, patient confidentiality, information security and rights of access to information.

2.6 The Head of Electronic Systems & Records & Records Manager is responsible for records management within the Trust and for monitoring compliance and effectiveness of this policy. They are the responsible officer of this policy.

2.7 It is the responsibility of all staff including contractors and third parties to comply with this policy in carrying out their duties within the Trust and for bringing any areas of non-compliance or queries on its application to the attention of their line manager.

2.8 The Information Governance Steering Committee (IGSC) is a multi-disciplinary committee that is responsible for overseeing records management and advising on local policies relating to retention, archiving or disposal of sensitive, personal health / social care or corporate records, and ensuring that adequate resources are available to meet the Trust’s obligations and that policies and procedures are adhered to.
3.0 DEFINITIONS

3.1 All NHS records are Public Records and must be kept in accordance with the following statutory and NHS guidelines:

- Care Quality Commission – outcome 21
- The Freedom of Information Act 2000
- Data Protection Act 2018

3.2 The Trust creates, receives and maintains records and information covering a wide range of activities, subjects and actions. Records and information may relate to patients, staff, financial transactions, strategic planning, daily operations, policies and procedures.

3.3 It is likely staff will receive requests for information and/or copies of records from patients, external institutions or members of the public. For example:

- A patient may request to see his/her patient records
- Relatives of a patient may request to see his/her records
- A member of the public may request to see a copy of a Trust policy document
- A research organisation might request some statistics on hospital admissions
- A member of staff may request to see what is written about them in an appraisal

3.4 Requests may be received for both confidential and non-confidential information

3.5 A record is: any information held on any format e.g. electronic systems, paper, CD, microfilm including (Health and Social Care records and Corporate records)

**Written**

For the purposes of this policy the term ‘written’ denotes a tangible copy; which must be printed matter from the Trust’s electronic system, typed documentation or handwritten documents.

**The unified health and social care record**

A completely unified health and social care record that comprises all of the demographic, social care and clinical care information for a patient/service user’s care pathway. If paper, there may be more than one volume comprising the unified health and social care record for a patient/service user.
### The subsidiary record
A health and social care record that is maintained in parallel to the unified health and social care record, when there is more than one mental health service being delivered to a patient/service user and the records are in a paper format.

### The electronic unified health and social care record system
The complete and identifiable health and social care record for a patient/service user held in electronic form; which provides 24 hour access to authorised practitioners and staff.

### Social care record
A record created and held by social services staff.

### Person identifiable
Containing any information from which a person will be identified – for example: patient/service user or carer’s name, initials, address (including postcode), date of birth etc.

### Casenote architecture
The physical format of the paper unified health and social care record, including instruction of what is to be filed and where. In electronic records a relevant tab structure and storing process is established and shared.

### 4.0 PRINCIPLES
- To support the guidelines contained in the Information Governance Alliance – Records Management Code of Practice for Health and Social Care Records 2016
- To identify the way in which the management of records in the Trust is currently structured.
- Accountability – to ensure accurate records are maintained for legal, audit or examination purposes.
- To provide documented retention and disposal schedules to include provision for permanent preservation of archival records.

### 5.0 RECORDS PROCEDURES

#### 5.1 Records Management Lifecycle

Records lifecycle in records management refers to the following stages of a records "life span": from its creation to its preservation (in an archive) or disposal.

- **Create**
- **Index**
- **Store**
- **Retrieve**
- **Archive**
- **Preserve**
- **Dispose**

---

Page 7 of 29
5.2 Records Creation

5.2.1 The content of a record will primarily be determined by the purpose for which it is being created, for example a personnel file will contain information about an employee relating to things like employment history etc., a patient’s medical file will contain information about diagnosis and treatment.

5.2.2 Records of business activity should be complete enough to:

- Facilitate an audit or examination of the business
- Protect the legal and other rights of The Trust, its patients and any other person affected by its actions
- Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

5.3 Records Storage

On-site

North Locality

5.3.1 Hard copy Medical Records are stored in the main libraries Langdon Mental Health Unit, Basildon / The Derwent Centre and other outpatient satellite storage areas within North Essex locality.

5.3.2 Electronic Medical Records stored or generated within Mental Health are stored on Paris and on Theseus for substance misuse.

5.3.3 Departmental non-clinical records are stored locally within each section and in on-site storage areas – details of these records and their locations can be found within the Information Governance Team via their information asset register.

South Locality

5.3.4 No hard copy active medical records exists within the organisation.

5.3.5 Electronic medical records stored or generated within the community teams are stored on SystmOne, for Mental Health on Mobius and Theseus for substance misuse service.

Off-site

5.3.6 Offsite storage is managed by external contractors, currently both North and South Locality including Bedfordshire all have separate external contractors – they offer active storage, semi-active storage and deep storage. Requests for records to be sent offsite and or retrieval must go through email - epunft.essex.records@nhs.net.
5.3.7 Records archived with the external contractors should be fully indexed and referenced to the box and should be sent with a review/destroy date (in line with The Trust retention schedule) clearly identified.

5.4 Records management / keeping

5.4.1 The importance of good record management cannot be underestimated. It ensures that:

- All records created are of the highest quality; are accurate, clear and relevant and meet required standards of data quality
- Records are always accessible, and staff in the organisation are able to work with maximum efficiency without having to waste time hunting for information
- There is an “audit trail” which enables any record entry to be traced to a named individual at a given date-time with the secure knowledge that all alterations can be similarly traced
- Those needing to read records at a later date can see what has been done, or not done, and why
- Any decisions made can be justified or reconsidered at a later date

5.4.2 In addition, the Trust recognises the need to manage records properly to:

- Support patient care and continuity of care
- Support day to day business which underpins delivery of care;
- Support evidence based clinical practice;
- Support sound administrative and managerial decision making, as part of the knowledge base for NHS services;
- Meet legal requirements, including requests from patients under access to health records legislation;
- Assist health and other audits; and
- Support improvements in clinical effectiveness through research and also support archival functions by taking account of the historical importance of material and the needs of future research.

Record Keeping

5.4.3 High quality record keeping is one of the main components of Clinical Governance and we must ensure that health and social care records made by staff within the Trust are of consistent quality. This will be achieved by:

- Establishing and maintaining consistent standards of record keeping throughout the Trust
- Ensure all clinical records comply with professional standards and those of accreditation bodies i.e. GMC, NMC
- Ensure that record keeping meet legal obligations
- Ensure that the Clinical Governance requirement for effective monitoring of clinical care and high quality record keeping are met
- Meet Information Governance Toolkit Standards
- Support evidence based clinical practice and improvements in clinical effectiveness
• Ensure that the requirements under the Research Governance Framework for effective monitoring of research related record keeping are met

Legal Obligation and Good Practice

5.4.4 Although the primary purpose of health records is to facilitate continuity of care and to act as a tool of communication, good records allow a clear picture of events to be obtained which is vital for legal or evidential reasons. Records must be objective and worthy of independent scrutiny – in the event of an investigation their content can be critical.

5.4.5 The approach to record keeping which courts of law adopt tends to be that ‘if it is not recorded, it has not been done’

Documentation and Professional Accountability

5.4.6 All healthcare practitioners and staff involved in clinical care or undertaking research are professionally accountable for keeping clear, legible, accurate and contemporaneous clinical records which record all the relevant clinical findings, any decisions made, information given to patients and any drugs or other treatment prescribed.

5.4.7 All clinicians have both a professional and a legal duty of care to patients. All professional organisations will expect that high quality standards of care including record keeping are maintained. Record keeping standards are an indication of professional practice.

5.4.8 A health record should inform any clinician who has a responsibility for the patient of all the key features which might influence the treatment proposed. It should also provide a contemporaneous and clear record of the patient’s treatment and related features. A good record speaks volumes about the care a patient has received, and has a vital role in minimising clinical risk.

5.4.9 Good record keeping safeguards both patients and professionals from unsafe practice through the misrecording or misunderstanding of health record information.

5.4.10 For clinical records the purpose is to facilitate care, treatment and support of a patient or patient/service user. Therefore, these records should:

("be typed” means directly into an electronic system using the appropriate forms)

• Include demographic, clinical and social care information
• A record of assessment of risks and needs
• Evaluations of care and treatment
• Progress under CPA or other care plan arrangements
• Results of biochemical and other tests if any
• Prescription and administration of medication if any
• The recording of detention under the Mental Health Act 1983 as amended by the Mental Health Act 2007 if any
Identify who has been responsible for which aspects of care and treatment
Identify when care and treatment was given.

And also be:

- Be factual, consistent and accurate
- Where paper exists - be written in black ink, with the exception of pharmacy which will be in green for verification purposes.
- Be typed / written as soon as possible after the event has occurred, providing current information on the care and condition of the patient/patient/service user (if the date and time differs from that of when the records are written up, this should be clearly noted under the signature, printed name and position/grade.
- Be typed / written clearly, legibly and in such a manner they cannot be erased (electronic records once saved cannot be erased) Where paper exists erasers, liquid paper, or any other correction fluids should not be used to cancel errors.
- A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment. In electronic records the above principle is applicable for use within the continuation sheets.
- Be accurately dated, timed and signed electronically in line with both Information Governance and ITT policies and procedures The use of abbreviations should be kept to a minimum
- Be typed / written, wherever possible, with the involvement of the patient/patient/service user or carer and in terms that can be understood by all
- Be contemporaneous and continuous, with electronic records all documents saved will be in a time line effect.
- Documents must be inputted into the electronic system as soon as possible and saved. Printed documents and / or hand written documents must be scanned within a 24 hour period. (Weekends and bank holidays will be the exception)

5.4.11 Records must not contain:

- Information that is not relevant to the patient / patient/service user to whom the record/s pertains
- Opinions that are not professionally based
- More than one copy of any document, although duplicate letters should be retained if they are date-stamped as being received by different people.

5.4.12 Good Record Keeping Ensures That:

- Staff can work with maximum efficiency without having to waste time searching for information
- Any record entry or alteration can be traced back to a named individual at a given date/time
- Those caring for the patient after you can see what has been done, and still needs to be done and the reasons for this
• Any decisions made can be justified or reconsidered at a later date if the situation changes

5.4.13 Relevant and Useful

- Identifying problems that have arisen and the action taken to rectify them and expected outcomes
- Providing evidence of the care planned, the decisions made, the care delivery and the information shared
- Providing evidence of actions agreed with the patient/service/user (including consent to treatment and/or consent to share information)

5.4.14 And Including

- Clinical observations: examinations, tests, diagnoses, prognoses, prescriptions, other treatments
- Relevant disclosures by the patient/patient/service user (likely to understanding cause or effecting cure/treatment)
- Facts presented to the patient/patient/service user
- Correspondence from the patient/patient/service user or other parties
- Patient/patient/service user to write an account of their illness in their records, ensuring this is on a separate sheet of paper, their name is clearly identified as the author, it is dated and signed.

5.4.15 Patient/Service user Records Should Not Include

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subject statements
- Personal opinions regarding the patient/patient/service user (restrict to professional judgements on clinical matters)
- The name(s) of third parties involved in a serious incident. The name should be included on the separate incident form for cross referencing
- Detailed correspondence generated from legal papers and complaints

5.4.16 Litigation and Complaints and Data Protection requests

5.4.16.1 Correspondence generated from patient/patient/service user litigation and complaints must not, under any circumstances, be filed within the clinical records. These documents are not relevant to clinical care and are often restricted from disclosure, unlike the clinical record itself.

5.4.16.2 However, when a report is generated to assist in a legal case, this may be relevant to clinical decision making, or documents pertaining to the formal admission of patients under the Mental Health Act 1983, and may be filed within the clinical record.
5.4.17 Health Record Keeping Standards

5.4.17.1 The Trust audits against standards and requirements set by national, professional and accreditation bodies.

5.4.17.2 The Trust recognizes that there are two main areas in developing standards for clinical records and they are in generic and professional quality.

5.4.17.3 Generic quality is concerned with the basic content and structure of the record. Professional quality relates to the value of the record as an effective communication tool.

This above is a statement of good-practice principles, and is not intended as a comprehensive list of standards.

5.5 Record Creation/Registration/Architecture

5.5.1 This is the complete record either paper or electronic of each individual patient / patient/service user and can be kept in one or more volumes (paper).

5.5.2 Records are created to ensure that all information is available within the Trust:

- To support the care process and continuity of care
- To support the day-to-day business, which underpins delivery of care
- To support evidence based practice
- To support sound administrative and managerial decision making
- To meet legal requirements, including requests from patients/patient/service users and staff under the Data Protection Act 2018 and Access to Health Records (pertaining to deceased individuals only)
- To assist in health and other audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of media and the needs of future research
- Whenever and wherever there is a justified need for information, and in whatever media it is required

Registration

5.5.3 In order to ensure records can be identified and retrieved when required it is necessary to allocate a unique number via a registration system to records.

5.5.4 The types of records, which are most likely to be placed on a registration system, include:

- Clinical / Health and Social Care records
- Personnel records
- Financial records/papers
- Performance monitoring
- Policy papers (reports, correspondence, etc.)
- Minutes, circulated papers etc. of meetings
• Papers relating to the preparation of legislation
• Complaints papers and correspondence
• Research and development papers

North Locality

It must be noted that the Trust is paper-lite in the South and working towards this for the North; firstly the inpatient units followed by the community teams; therefore no new volumes should be created after the Paper-lite project has been implemented.

5.5.5 All paper health and social care records must be recorded and electronically tracked on the Trust’s information system; these will be identified with a case note type ‘Main’. All practitioners and administrative staff must use it and keep it up to date. This must also identify the correct volume number i.e. (Main 1, Main 2 etc.) both on the cover of the record (Blue files) and on the relevant tracking system.

5.5.6 Senders must ensure notes are tracked out at appropriate date, time and destination. The recipient must track the notes into their new location, identifying the holder’s name and the accurate date and time they were received.

5.5.7 The staff member to whom the unified health and social care record is tracked out to will always be the first person to be approached should loss of the unified written health and social care record is suspected.

5.5.8 The geographical spread of the teams and facilities means that maintenance of a true single health and social care record, where all information pertaining to an individual patient / patient/service user is held in one file, is not always feasible. The teams and practitioners are therefore able, when appropriate; to create a subsidiary record that exists in parallel with the unified health and social care record for as long as the team or practitioner is involved in the care of that individual. These subsidiary records must be recorded and tracked on the electronic systems. These will be identified with a case note type of ‘Subsidiary’. This must also identify the correct volume number i.e. (Sub 1, Sub 2 etc.)

5.5.9 The Trust’s practitioners must be aware of the existence of written Social Care records held by Essex County Council relating to the social care received by a patient/service user prior to the formation of the Partnership Trust, or social care that was not related to mental health difficulties. Practitioners must use the Paris/SWIFT interface to ascertain if this is the case and liaise with their social services colleagues to ensure they have all the information available to provide a seamless service to the patient/service user.

5.5.10 In addition, it must be observed that social workers within older adult services are not seconded to the Trust and in these instances for those patient/service users that have a social worker nominated as their CPA care coordinator/Lead Professional and who primarily have a social care need, there will be a separate Essex County Council social care record in existence.
5.5.11 When a patient/service user is in contact with more than one of the Trust's services, it will be necessary to create subsidiary records. In these instances the unified health and social care record must be held by the CPA care coordinator or the health care professional deemed most appropriate to hold them, this will be discussed and reconsidered at each of the patient/service users' CPA reviews. The exception to this rule is when the patient/service user is an inpatient; in those cases the inpatient ward must hold the unified health and social care record.

**South Locality**

5.5.12 All records created within Mental Health (Mobius) Community Services (SystmOne) and substance misuse (Theseus) are directly created within the electronic systems. Therefore the unique identifier is allocated automatically.

**Architecture**

**North Locality**

5.5.13 The paper unified health and social care record is produced with sub-dividers appropriate to all the various requirements of the Trust's provisions, therapies and treatments. On the inside cover of the record are comprehensive instructions to assist the user to file all documentation correctly.

5.5.14 The filing of documents in the unified health and social care record must adhere to the following:

- Documentation is filed behind the correct divider
- Documentation is filed in strict chronological order, with the most recent on the top.
- Paris generated or hand written clinical notes are filed in narrative order, with the most recent at the bottom.
- All documentation is filed using the file's binding/fixing system, and none is kept loose or in pockets.
- Documentation is filed the right way round and the right way up.
- The Trust's practitioners and other staff using unified health and social care records, who identifies that any of these principles is not adhered to must rectify the situation themselves.

5.5.15 When a patient/service user’s record becomes full, typically 2 inches thick, a new volume must be raised. This is irrespective of it being a Main record or a Subsidiary record; although if it is a Subsidiary record it is preferable to slim-down the record by reviewing the contents and sending some of the supplementary paperwork to the holder of the unified health and social care record (Main) for incorporation; whilst retaining the relevant and key information required to provide safe, risk free care to the patient/service user.

5.5.16 It is recommended as good professional practice that all original assessments, risk assessments and other key information must be copied and transferred into any new volumes of records for a patient/service user. Ensuring that vital information about a patient/service user is not lost or overlooked due to the passage of time.
5.5.17 If the holder of a subsidiary record discharges a patient/service user, the subsidiary record will be sent to the holder of the unified health and social care record, typically this will be the CPA care coordinator. He/she, or an administrator working on their authority, will incorporate all the material in the subsidiary record within 5 working days of receiving it, ensuring that no more than one copy of any particular document exists.

5.5.18 The holder of the unified health and social care record will identify on the Trust’s Paris electronic recording system that the subsidiary record has been incorporated.

South Locality

5.5.19 The electronic records systems already have established agreed document structures. Any changes required to these structures would need to go to the relevant project boards for a decision.

5.6 Accessing Records/Security/Confidentiality

5.6.1 Access and use of records containing person identifiable material is governed by the Data Protection Act 2018, the Access to Health Records Act 1990 and Caldicott Principles.

5.6.2 Confidentiality levels bind all Trust staff. Managers must therefore ensure that all staff are trained in data protection and are aware of the implications should confidentiality be breached. The impact of a breach of confidentiality could be any of the following:

- Threat to personal safety or privacy
- Embarrassment for the Trust
- Legal obligation
- Financial loss
- Disruption of activities

Staff do not have an automatic right to look at their own health records or those of colleagues, friends and family, they too must follow this procedure, failure to do so will be considered an Information Governance breach.

5.6.3 The Trust is committed to multi-disciplinary working procedures and this requires all key professionals to work together and share information to the benefit of the patient/client. Patients/clients have an expectation that information held relating to them is confidential and held securely and will be available to facilitate and inform their care and to assure their safety and that no unauthorised person will be allowed deliberate or inadvertent access to the confidential information contained in the unified health and social care record or subsidiary record.

Accessibility to Health and Social Care Records Process

5.6.4 Within the clinical capacity the transfer of clinical records between clinical environments is essential to the provision of appropriate care and treatment. The record must be transported as little as possible, but when it is necessary, it must be by the most secure means available. It is essential that the
required Directorates have in place appropriate mechanisms and protocols to ensure the secure transfer of clinical records.

South Locality

5.6.5 Records can be accessed 24 hours per day, 7 days per week, via the Trust’s electronic patient records systems. HIE is available to staff to improve patient care and decision making by facilitating the safe sharing of patient records and vital information, which is both easily accessible and relevant.

Reducing the time and removing challenges that can be faced by clinical staff when retrieving patient information. However if paper files do exist then the following applies:-

- 9.00am – 5.00pm, Monday to Friday – contact to be made with the epunft.essex.records@nhs.net to retrieve the relevant record from offsite storage providers
- Bank Holidays and Weekends – as above
- Electronic paper based records are available at the desk top 24-7. Authorised staff have access to the electronic system. Each ward and team has been given guest log in access if additional access is required both during hours and out of hours. For detailed instructions on electronic retrieval please refer to procedure CPG9(d)

5.6.6 Records stored offsite are retrieved on a daily basis and are delivered within 24 hours to a designated location.

- 9.00am– 5.00pm, Requests for records are sent to delegated records staff who liaise with the offsite storage provider. Records are returned to a designated location and then forwarded on to the original requester. All records are tracked both at the offsite storage provider and on the Trust’s internal catalogue
- 5.00pm – 9.00am plus Bank Holidays and weekends, notes required urgently and in cases of extreme emergency, may be retrieved through the contact centre who will liaise with the designated out of hours staff. The Service level agreement with the offsite storage provider allows records to be delivered within a 2-4 hour time frame. All records are tracked both at the offsite storage provider and on the Trust’s internal catalogue

North Locality

5.6.7 Records can be accessed 24 hours per day, 7 days per week, via the Trust’s electronic patient records systems. HIE is available to staff to improve patient care and decision making by facilitating the safe sharing of patient records and vital information, which is both easily accessible and relevant. Reducing the time and removing challenges that can be faced by clinical staff when retrieving patient information. However if paper files do exist then the following applies:-
- There are 24 hour-a-day retrieval systems in place, where 24-hour mental health services exist, i.e. inpatient wards. Only those practitioners involved in a patient/service user's care will be able to access that patient/service user's unified written health and social care record.

- Records will be kept securely at the facility or facilities from which the patient/service user is receiving that care. After use, and at the end of the working day, the unified health and social care records and any subsidiary records that exist, must be locked away in secure filing cabinets, in lockable offices away from public areas, in safe fire and intruder alarmed surroundings.

- When a patient/service user is discharged from the mental health services, the unified health and social care record will be returned to the medical records library, or other approved archive, within 15 working days of post discharge for secure storage. Unified health and social care records in medical records libraries will be filed in secure racking, in safe fire and intruder alarmed surroundings, using the clear terminal-digit filing system.

- The unified health and social care record will be retrieved and dispatched from medical records libraries on the day of the internal request (i.e. a request from within the Trust) is received. This standard will apply on requests received until 1 hour before the end of the usual working day.

- When a patient/service user is admitted to an inpatient ward it is essential that the unified health and social care record is made available to the ward staff as soon as possible or within 24 hours.

- When a patient/service user is discharged from an inpatient ward to a community, day or outpatient service, it is essential that the transfer of the unified health and social care record is made to the named CPA care coordinator within 5 days of the discharge.

- At the end of an episode of care, the subsidiary record must be sent to the holder of the unified health and social care records for incorporation. There must not be any subsidiary records existing for a patient/service user after their discharge from mental health services. Medical records libraries will only store unified health and social care records.

- The health care professional holding the unified health and social care record, or an administrator working on their authority, must incorporate a subsidiary record they have received, into the unified health and social care record within 5 working days of receiving it.

- The unified health and social care record in general must contain no more than one copy of any particular document, although duplicate letters must be retained if they are date-stamped as being received by different people.

- Where local arrangements exist and record storage takes place outside medical records libraries, for example in any other...
approved archive or local secure storage facility, the same provisions apply.

- Where more than one mental health service is involved and subsidiary records exists, professionals will need to communicate regularly to ensure there are no gaps in the delivery of care. Each of the professionals involved and holding Main or Subsidiary records for a patient/service user; must copy summaries of care, including risk assessments, discharge summaries, important letters and results at least every 3 months; or more frequently when deemed clinically necessary. This is in addition to the patient/service user’s CPA review process.

**Accessibility to In-Patient Records – Out-Of-Hours**

5.6.8 Inpatient clinical records should be accessible throughout the period for which the patient is resident within the Trust. In addition, records should be retrievable for all new patients admitted, irrespective of their arrival day or time.

**Subject Access Requests – Clinical Records**

5.6.9 Under the Data Protection Act 2018, the following individuals are entitled to have access to their clinical records (subject to some safeguards and exceptions), regardless of when the record was created, providing consent and required documentation is received:

- The patient/service user
- A person authorised in writing to make an application on the patient/service user’s behalf
- A person with parental responsibility when the patient/patient/service user is a child
- A person appointed by the court to manage the patient/service user’s affairs because of incapability

5.6.10 Solicitors needing access to the records will need the consent of the patient/service user prior to any access being granted

5.6.11 There are some exceptions where records can be shared without patient/service user consent:

- The Mental Health Act Commission when patient/service users are detained under Mental Health Act 1983 as amended by the Mental Health Act 2007
- The General Medical Council - if a doctor is under investigation
- The police - if someone is at serious risk or a serious crime has been committed
- The courts - in criminal or other legal cases, when a court order is made
- Child Protection staff - where there is concern over a child’s welfare and safety (even if the child is not under our care). Staff have a duty to volunteer information before it is asked for if they suspect a child is at risk.
• The DVLA - if a patient/service user's illness might make it unsafe for them to drive.

5.6.12 Under the Access to Health Records Act 1990, the following individuals are entitled to have access to the clinical records of deceased patients/service users:

- The personal representative of the deceased patient (e.g. the Executor of the Estate)
- Any person who may have a claim arising out of the patient’s death

5.6.13 Patients/service users wishing to make subject access requests should be directed to the Trust’s Records Manager using the following email address: epunft.accesstorecords@nhs.net

5.6.14 Under the terms of the same legislation, individuals also have a right to have their unified health and social care records amended if the records contain inaccuracies, misrepresentations or errors of fact. The Trust and its practitioners therefore have a duty to ensure that what is written in the unified health and social care record is accurate, to-the-point and as far as possible objective.

Subject Access Requests (Corporate Records)

5.6.15 Under the Data Protection Act 2018, members of staff are entitled to see their own personnel records. Staff wishing to request formal access to their records should contact the Trust’s Legal Department

Access to Corporate Records

5.6.16 The Freedom of Information Act (FOIA) 2000, which came into force in January 2005 was designed to ensure greater openness within the public sector, a commitment that is thoroughly supported by the Trust. The Act grants members of the public access to all types of recorded information that is held by the Trust.

5.6.17 The Trust has established efficient and effective procedures to ensure that requests for information under the terms of the FOIA are managed and actioned appropriately. Further information in relation to these procedures can be found within CP/CPG25 – Freedom of Information 2000 Policy and Procedures.

5.6.18 Certain information may be exempt from disclosure, under one or more of the 23 exemptions. For example, the disclosure of personal or private information relating to an individual is forbidden under Section 40 – Personal Information.

5.6.19 Under the terms of the FOIA, the Trust has developed a publication scheme that is available via its website www.eput.nhs.uk. Any requests for information from the publication scheme must be forwarded to the Legal Team.
5.6.20 Any applications for information made under the FOIA, which have been received by staff must be forwarded immediately to the FOI team epunft.foi@nhs.net

5.7 Electronic Records Systems

5.7.1 The Trust is committed to reducing clinical risk to patient/service users by ensuring that their staff benefits from having as much information about them as possible prior to caring for them. To achieve this, the Trust has mandated the complete use of electronic systems for recording all patient/service user demographic, clinical and social care information. To speed up the process of loading a document, some documents may be archived from the patients Mobius file – the Archive Restore form should be used to retrieve these documents.

North Locality

- The primary electronic system used by the Trust is Paris.
- The Theseus system is used within the substance misuse services, although CPA and unified health and social care record tracking is recorded on Paris.
- The SWIFT system is used in conjunction to Paris by those social services staff that are not seconded into the Trust, but who work closely within the older adult community based teams. Data entry onto SWIFT should be made only where functionality does not exist within the Paris system, for example where packages of care are funded and delivered within social care. It is recognised this will result in some duplicated data entry.
- SystmOne is used by the local GP’s.

5.7.2 From the point of a patient/service user’s external referral being received, throughout the mental health and social care pathway to their discharge, all demographic, clinical and social care activity must be recorded on the Paris system.

5.7.3 All the care activity for a patient/service user recorded on the Paris system must be printed and appropriately filed within the patient/service user’s unified health and social care record. This will provide continuity for the patient/service user and ensure that all information is made available to staff whether they are viewing the unified health and social care record or viewing the Paris electronic record system.

5.7.4 The existence of unified health and social care records or subsidiary records must be identified and tracked on the Paris electronic system, ensuring that patient/service users and staff are not put at risk.

5.7.5 All staff must make themselves fully aware of the Paris policy and Paris guidelines that can be found on the Trust’s intranet site.

5.7.6 All patient/service users referred to the substance misuse services will have their demographic, CPA details and case note tracking recorded on the Paris electronic system; however, the patient/service user care pathway through
substance misuse services will be recorded on the Theseus electronic system.

5.7.7 For those patient/service users referred to the older adult community mental health teams, who have a social worker as their CPA care coordinator and who primarily have a social care need; will have their care pathway recorded on Paris and their social care need details will also be recorded on the SWIFT electronic recording system. This would typically be when packages of care are required to be recorded as this has to take place on the SWIFT system and will involve some replicated data entry.

South Locality

5.7.8 The primary electronic system used by the Trust is Mobius for Mental Health, SystmOne for Community services and Theseus for substance misuse.

5.7.9 The use of information technology is increasing within the NHS generally and a large proportion of documents are now produced electronically. This change places new demands on the managing of records. For example, if an electronic document is to be produced as evidence in court cases it will only be accepted if assurances can be given that the Unified Electronic Patient Records System (UEPR) was not being misused and was operating properly at the time the record was produced.

Scanning/Access Control

5.7.10 For reasons of business efficiency the Trust has undergone the transition of scanning archived health records into electronic records, which exist in paper form. All new patients/service users records are electronic from the point of contact with the Trust.

5.7.11 The UEPR will provide an authentication mechanism that controls access to its information and that validates each user attempting access at the start of each user session. Each user will enter a unique user-name and password in order to gain entry to the system.

Managing the Electronic Record

5.7.12 The Trust will monitor electronic records to ensure that:

- Records to be captured are being processed electronically if they do not appear in the paper record
- As far as possible, there is no duplication between the paper and electronic records
- A distinction is made between printed electronic records and those, which reside in the paper record
- An inventory is kept of all records that are scanned electronically
Standards for Electronic Records

5.7.13 The principles for electronic record keeping are the same as for paper records. In addition, when using electronic documentation, the Trust will ensure that the following procedures are in place, including:

- Physical/equipment security
- Access control
- User password management
- Computer virus control
- Data backup
- Computer network management
- Data and software exchange
- Validation
- Adequate training for all users

Security of Electronic Records

5.7.14 The Trust must implement and maintain an electronic records security program for office and storage areas. Any software or documentation required to maintain the functionality of the UEPR equipment must be located in a separate building. If records are stored on rewritable electronic media, the UEPR system must ensure that read/write privileges are controlled and that an audit trail of rewrites is maintained.

Maintenance of Electronic Records

5.7.15 The Trust should maintain all long-term and permanent backup and security electronic recording media in a storage facility, either on-site or off-site, with the correct temperature and relative humidity controls (i.e. temperature below 70 degrees Fahrenheit, and humidity 30 to 40 percent).

5.7.16 The Trust should carry out an audit annually to read a statistical sample of all electronic media to identify any loss of information and to discover and correct the cause of data loss. The Trust should also consider the necessity to copy the media, after a specific agreed time period, and transfer onto tested and verified new media. This will ensure that enough ‘memory core space’ within the ERMS is available.

Legal Admissibility

5.7.17 All scanned records will be copied and stored in accordance with British Standards, in particular the ‘Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically’ (BS 10008). This provides good practice guidance on the electronic creation, storage and retrieval of information, duty of care, audit trails, and records management requirements for electronically stored information. Non-compliance could have a major impact on information being accepted in a court of law.

5.7.18 In order to ensure that this need is met, records should be stored on network drives and not on individual hard drives (C:\ or any folder beginning with ‘My’). The policy on encryption of memory sticks must also be adhered to when using this media.
5.8 Retention and Destruction

Retention

5.8.1 The Public Records Act 1958 imposes a statutory duty of care upon all individuals who have direct responsibility for any such records. The Trust follows the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016. These are recommended minimum retention times from the Information Governance Alliance, although where there is a business need, records may be retained for longer periods. Where this is the case the decision must be justifiable.

Retention of Electronic Records

5.8.2 The retention criteria for electronic records are the same as for paper records. This retention criterion will include provisions for:

- Scheduling the retention and disposal of all electronic records, with the approval of the Trust Electronic Records Group and / or the Information Governance Steering Committee
- Establishing procedures for regular recopying, reformatting and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorised life cycle

5.8.3 Electronic records must be destroyed in accordance with the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016. At a minimum the Trust should ensure that electronic records scheduled for destruction are disposed of in a manner that ensures protection of sensitive personal information.

Selection of Paper-Based Records for Permanent Preservation

5.8.4 All NHS records, whether paper-based or electronic, are public records under the terms of the Public Records Act 1958.

5.8.5 Prior to the decision to destroy any paper-based record, the Trust will give consideration to the value of the content to future generations and may take into account any genetic implications. Records which are thought to be worthy of permanent preservation, should be referred to the Trust Electronic Records Group and / or the Information Governance Steering Committee for review, whereby arrangements for their deposit in a place appointed under the Public Records Act 1958 will be made.

Disposal, Destruction and Destroying

5.8.6 Disposal is defined as the point in a records lifecycle when they are either transferred to an archive facility or prepared for destroying.

5.8.7 Destroying is defined as where the records are no longer required to be kept due to statutory requirement or administrative need and they have no long-term historical or research value.
5.8.8 Destruction is defined as the definitive obliteration of a record beyond any possible reconstruction.

In conjunction with this policy please also refer to Storage, Retention and Destruction procedure CPG9(c) Electronic Records Procedure CPG9(d) and Secure Handling and Disposal of Confidential Waste procedure RMPG13(d)

5.8.9 All Clinical records contain sensitive and confidential information. It is vital that confidentiality is safeguarded at every stage of disposal and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will mean disposal as confidential waste, in confidential waste bags provided throughout the Trust or by use of confidential ‘waste bins’. It is important to remember that the destruction of records is an irreversible act. It is important to note that ‘recycling’ bins do not provide a safe destruction method.

5.8.10 The Trust uses contract services for the transporting and destruction of certain records, namely clinical records. The Contract terms must include guarantees on security and confidentiality of information. Enquiries regarding this should be addressed to the Records Manager in the first instance. A register of records destroyed should be kept, recording what was destroyed, when and by whom.

5.8.11 Managers must ensure that corporate records held within their areas of responsibility that are no longer required for business use are reviewed as soon as practicable under the criteria set out in Information Governance Alliance Guidance for records.

5.8.12 Only the Head of Electronic Systems & Records / Records Manager has the authority to action records for destruction. Individual staff members are only permitted to destroy individual paperwork which includes duplicate reports, version controlled / draft documents and letters. Please always check with your line manager prior to any destruction.

5.8.13 In line with the policy for the destruction of records, patient/service users with an identified diagnosis of one of the following will not be destroyed and marked as such:

- Huntington’s Chorea F022
- Creuzfeldt Jakob’s Disease F021
- Pick’s Disease F020
- Parkinson’s Disease F023
- Human Immunodeficiency Virus F024

Specific Clinical Records Destruction

5.8.14 Please refer to storage, Retention and Destruction procedure CPG9(c) and Electronic Records procedure CPG9(d) for further guidance.
Destruction Process

5.8.15 All records are reviewed in accordance with both the Information Governance Alliance - Records Management Code of Practice for Health and Social Care 2016 or Trust procedure CPG9(c) Storage, Retention and Destruction of Records Procedure.

5.8.16 Individual departments all have the facility for local blue bin destruction which is then periodically collected and shredded on site with approved contractors.

5.8.17 The destruction of clinical/health records only takes place via the scanning department in conjunction with the Trust’s Head of Electronic Systems/Records, once process as outlined in CPG9(d) Electronic Records Procedure has been followed. The Information Governance Steering Committee has given prior authority for these records to be destroyed.

5.8.19 Specific destruction requests are made with the approved contractors for bulk destruction.

5.8.20 In all cases destruction certificates are obtained.

5.8.21 For records stored in offsite storage facilities (corporate only) a concise catalogue is kept with retention dates, these are looked at periodically. Any box numbers identified that require destruction are returned to the originating department for approval. Once this approval is received the Trust’s Head of Electronic Systems/Records will instruct the offsite storage provider. Checks are made against each of the box numbers and once satisfied authorisation is given from the Trust to destroy. A destruction certificate is then obtained.

5.9 Storage

5.9.1 The Trust has a responsibility for ensuring the effective and efficient operation of all storage facilities within the organisation. This includes the safekeeping, accessibility and retention of records for as long as required, the transfer of those records selected for permanent preservation, and the timely destruction of records no longer required.

5.9.2 All storage facilities should be in a suitable environment, which has easy access and appropriate safety to ensure the records are not damaged or destroyed.

Transportation

Please refer to the Trust’s Transfer Transportation procedure CPG9f

Emergency request for records

5.9.3 There will be the need from time to time to request records in an emergency situation (unplanned admission, no records at outpatient clinics, serious incidents) and records will need to be transported accordingly and securely.
5.9.4 All emergency records requests will still need to be tracked using the methods as described in this policy.

5.9.5 Approved carrier methods can be used i.e. couriers, internal postal collections, external approved taxis, providing the records have been secured in the first instance.

5.9.6 Any request from third parties including Police, Solicitors and Courts should initially be on an original request form and after authorisation from the on call director out of hours or the Access to Records Team during normal office hours, copies only of the records can be shared. Under no circumstances can the original record be given out.

5.9.7 Records required for serious incidents will in the first instance be photocopied and scanned and then sent and secured within the health records departments and before any further action can be taken or shared.

5.10 Sharing and Disclosing Information

5.10.1 The Trust will ensure appropriate agreements are put in place to govern the sharing of identifiable information between organisations. Such sharing must be in line with the care of the patient and the rights of staff in accordance with the Data Protection Act 2018.

5.10.2 Where information is requested in line with the Freedom of Information Act 2000, it will be managed in accordance with the Freedom of Information 2000 policy and procedures.

5.10.3 Where information is requested in line with the Data Protection Act 2018 it will be dealt with in accordance with their statutory right under the ‘subject access’ regime.

5.10.4 Requests for an individual’s health information will be dealt with in accordance with the Data Protection and Confidentiality policy and procedures.

6.0 MONITORING OF IMPLEMENTATION AND COMPLIANCE

6.1 The Director of ITT is responsible for monitoring the implementation and effectiveness of this policy and related procedural guidelines.

6.2 Monitoring of the availability of Clinical Records will be undertaken by the Trust’s Records Manager and any missing records will be reported to the Information Governance Steering Committee in the format of a report for action to be agreed.

6.3 A three yearly audit will be undertaken by the Information Department looking at the following:

- Roles and Responsibilities have been undertaken as outlined
- Legal Requirements have been met
• Process for tracking records has been followed
• Process for creating records has been followed
• Process for retrieving records has been followed
• Process for retaining and disposing of records has been followed

6.4 The quality of all written and electronic Clinical Records will be audited on an annual basis co-ordinated by the Clinical Audit Department.

6.5 Audits will be undertaken using the Trust agreed audit tools. The Quality Committee will be responsible for ensuring that the audit is undertaken annually, appropriate tools are used and action plans are developed and reviewed.

6.6 Results of all audits and monitoring will be presented to the Information Governance Steering Committee for review and an action plan development where necessary.

6.7 All audit reports will contain the background information on what was audited and why, outcome data for each element of the audit tool and recommendations and action plans for improvements.

6.8 The Workforce, Development and Training Department will undertake monitoring of training via OLM.

7.0 POLICY REFERENCES / ASSOCIATED DOCUMENTATION

7.1 The Trust is bound by a number of legislations governing an individual's rights, access to information, and the safeguarding of personal information concerning its patients and staff from unauthorised access and disclosure.

Legislation

- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 1992
- Human Rights Act 2000
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Copyright Designs and Patents Act 1988
- Children's Act 1998
- Public Records Act 1958
- NHS and Community care Act 1990
- Mental Health Act 1983 (revised 2007)
- Carers (Recognition & Service) Act 1995
- Patient/service users Access to Records Act 1987 and Regulations
- Adoption Act 1976
- Health Act 1999 (Section 31)
- Health and Social Care Act 2001
7.2 BS10008 is the British Standard that outlines best practice for the implementation and operation of electronic information management systems, including the storage and transfer of information. It is designed to help verify and authenticate all information to avoid the legal pitfalls of information storage. BS10008 outlines best practice for transferring electronic information between systems and migrating paper records to digital files. It also gives guidance for managing the availability and accessibility of any records that could be required as legal evidence.

8.0 REFERENCE TO OTHER TRUST POLICIES/PROCEDURES

Please read in conjunction with the following Trust’s policies, procedures and relevant legislation and guidance:

- Access to Records Procedure
- Freedom of Information Policy
- Data Protection & Confidentiality Policy
- IM&T Security Policy
- Transportation policy
INFORMATION GOVERNANCE AND SECURITY POLICY

POLICY REFERENCE NUMBER: CP50
VERSION NUMBER: 2
REPLACES SEPT DOCUMENT CP50
REPLACES NEP DOCUMENT Not applicable
KEY CHANGES FROM PREVIOUS VERSION GDPR compliant
AUTHOR: Information Governance Manager
CONSULTATION GROUPS: Information Governance Steering Sub-Committee, Quality Committee.
IMPLEMENTATION DATE May 2018
AMENDMENT DATE(S) Feb 2018: May 18 (GDPR)
LAST REVIEW DATE Feb 2018
NEXT REVIEW DATE February 2021
APPROVAL BY IGSSC March 2018
RATIFIED BY QUALITY COMMITTEE May 2018
COPYRIGHT © Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner.

POLICY 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 policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
The Executive Chief Finance & Resources Officer
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
</tr>
<tr>
<td>2.0</td>
</tr>
<tr>
<td>3.0</td>
</tr>
<tr>
<td>4.0</td>
</tr>
<tr>
<td>5.0</td>
</tr>
<tr>
<td>6.0</td>
</tr>
<tr>
<td>7.0</td>
</tr>
<tr>
<td>8.0</td>
</tr>
<tr>
<td>9.0</td>
</tr>
<tr>
<td>10.0</td>
</tr>
</tbody>
</table>
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
Computer Misuse Act (1990)
Electronic Communications Act (2000)
The Re-Use of Public Sector Information Regulations (2005)
The Civil Contingencies Act (2004)
The Copyright, Designs and Patents Act (1988) (as amended by the
Copyright Computer Programs Regulations (1992))
The Health and Safety at Work Act (1974)
Crime and Disorder Act (1998)
Health and Social Care Act (2000)
The Common Law Duty of Confidentiality
Integrated Governance Strategy
Information Governance Framework
Records Strategy
IM&T Security Policy
Data Protection and Confidentiality Policy / Procedure
Freedom of Information Policy / Procedure
Records Management Policy and related Procedures
Mobile Working and Remote Access Policy/Procedures
Data Quality Policy
Virtual Private Network Policy
Closed Circuit Television (CCTV) Policy / Procedure
Information Governance and Security Procedures
Paper and Electronic Corporate Records (Laserfiche) Policy / Procedures
IT&T Security Procedures
Internet/Email Access and Use Procedures
Information Sharing & Consent Policy / Procedure
This list is not exhaustive...

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

2.0 DUTIES / RESPONSIBILITIES

2.1 For the purposes of this policy, the definition of all staff includes all personnel
working for or with the Trust, or who have been authorised to access the
Trust’s information assets. This includes all management, permanent
employees, contractors, temporary staff, bank staff, locum, consultants, and
agents/agency employees (this list is not exhaustive).

2.2 All employees of the Trust, permanent employees, contractors, temporary
staff, bank staff, locum, consultants, and agents/agency employees (this list
is not exhaustive) are required to abide by the contents of this policy and its
associated procedural guidelines. Failure to do so may result in disciplinary
action.
Responsible Persons

2.3 Overall Responsibility Chief Executive

2.3.1 The Chief Executive has overall responsibility as accountable officer for the management and implementation of information governance / security for the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

2.3.2 As such the Chief Executive Officer signs up to the ‘Statement of Compliance’ declaration agreeing with its strict terms and conditions in relation to the security requirements for using N3 and for access to the Internet and NHS Connecting for Health applications.

2.4 Senior Information Risk Owner (SIRO).

2.4.1 The Chief Executive has delegated the day to day responsibility for information governance / security, policy and implementation to the Executive Chief Finance Officer as the Trust’s Senior Information Risk Owner (SIRO).

2.4.2 Making arrangements for information governance / security by setting / agreeing the overall policy for the Trust taking into account legal and NHS requirements.
   • Appointing the Information Governance Security Manager / key leads.
   • Appointing a Data Protection Officer to ensure that the provision of the Data Protection Act / GDPR is satisfied.
   • Ensuring that, where appropriate, staff receive information governance / security awareness and training
   • Chairing the Information Governance Steering Sub-Committee on a regular basis and through the Committee maintaining the Trust’s Information Governance / Security risk register and escalating any related risks to the Quality Committee

2.5 Caldicott Guardian

2.5.1 The Chief Executive has delegated responsibility for Caldicott issues to the Executive Medical Director, who is the Caldicott Guardian. The Caldicott Guardian has responsibility for reflecting patients’ interests regarding the use of their person identifiable information / data, together with ensuring that patient identifiable information / data is shared in an appropriate and secure manner.
2.5.2 The Trust has dedicated forums for the monitoring of Caldicott Principles through the:

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

who are responsible for:

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

2.6 Information Governance Manager

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

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

- 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 Common Law Duty of Confidentiality
- The Copyright, Designs and Patents Act (1990)
- The Health and Safety at Work Act (1974)
- 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 enquiries 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 – Email, Intranet, Internet Access & Use Procedure
CPG50C – Safe Haven Procedure
CPG50D – Information Security Incident Management Procedure
CPG50E – Data Privacy Impact Assessment Procedure
CPG50F – SMS Text Messaging to Service Users Procedure
CPG50G – Information Asset Register Procedure
CPG50H – NHSMail Usage Procedure
CPG50I – Not used
CPG50J – Information Governance Incident Reporting Procedure

END
APPENDIX 1

RISK PRIORITISATION SYSTEMS

The Trust’s Risk Registers are designed to assess the impact of identified risks on the Trust’s objectives and strategic plans. Each risk must be assessed in accordance with impact and likelihood of crystallisation and is then expressed in terms of a risk rating.

The wide variety of risks impacting upon the Trust ranges from those risks which threaten the achievement of the Trust objectives and those which impact mainly on individual Directorates / specialist committees. The potential impact of risks can therefore vary significantly and it is therefore necessary to have two scales for the assessment of impact – one scale for risks which are identified impacting on Trust Objectives and a second scale for those risks which impact on Directorate Objectives.

A.1 Risk Prioritisation for Risks of actions supporting Corporate Objectives

All identified risks emanating from high-level actions which support Corporate will be rated in accordance with the following process, as adapted from ‘A Risk Matrix for Risk Managers’ (NPSA):

A.1.1. Assess potential impact of risk on actions supporting Trust objectives and strategic plans

<table>
<thead>
<tr>
<th>Domains</th>
<th>Consequence score (severity levels) and examples of descriptors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Negligible</td>
</tr>
<tr>
<td>Impact on the safety of patients, staff or public (physical/psychological harm)</td>
<td>Minimal injury requiring no/minimal intervention or treatment.</td>
</tr>
<tr>
<td></td>
<td>No time off work</td>
</tr>
<tr>
<td></td>
<td>An event which impacts on more than 1 patient / member of staff</td>
</tr>
<tr>
<td></td>
<td>An event which impacts on more than 10 patients /staff</td>
</tr>
</tbody>
</table>
## INFORMATION RISK POLICY – CP57

<table>
<thead>
<tr>
<th>Quality/complaints/audit</th>
<th>Overall treatment or service suboptimal</th>
<th>Treatment or service has significantly reduced effectiveness</th>
<th>Non-compliance with national standards with signiﬁcant risk to patients if unresolved</th>
<th>Totally unacceptable level or quality of treatment/service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informal complaint/inquiry</td>
<td>Formal complaint (stage 1)</td>
<td>Formal complaint (stage 2) complaint</td>
<td>Multiple complaints/independent review</td>
<td>Gross failure of patient safety if findings not acted on</td>
</tr>
<tr>
<td></td>
<td>Local resolution</td>
<td>Local resolution (with potential to go to independent review)</td>
<td>Low performance rating</td>
<td>Inquest/ombudsman inquiry</td>
</tr>
<tr>
<td></td>
<td>Single failure to meet internal standards</td>
<td>Repeated failure to meet internal standards</td>
<td>Critical report</td>
<td>Gross failure to meet national standards</td>
</tr>
<tr>
<td></td>
<td>Minor implications for patient safety if unresolved</td>
<td>Major patient safety implications if findings are not acted on</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reduced performance rating if unresolved</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Human resources/organisational development/staffing/competence | Short-term low staffing level that temporarily reduces service quality (< 1 day) | Low staffing level that reduces the service quality | Late delivery of key objective/service due to lack of staff | Non-delivery of key objective/service due to lack of staff |
|                                                               |                                                                             |                                                        | Unsafe staffing level or competence (>1 day) | Ongoing unsafe staffing levels or competence |
|                                                               |                                                                             |                                                        | Low staff morale | Loss of key staff |
|                                                               |                                                                             |                                                        | Poor staff attendance for mandatory/key training | Very low staff morale |
|                                                               |                                                                             |                                                        |                                                                              | No staff attending mandatory/key training |

| Statutory duty/inspections | No or minimal impact or breach of guidance/statutory duty | Breach of statutory legislation | Single breach in statutory duty | Enforcement action |
|                            | Reduced performance rating if unresolved                      |                             | Challenging external recommendations/improvement notice | Multiple breaches in statutory duty |
|                            |                                                               |                             | Enforcement action | Prosecution |

| Adverse publicity/reputation | Rumours | Local media coverage – short-term reduction in public confidence | Local media coverage – long-term reduction in public confidence | National media coverage with >3 days service well below reasonable public expectation |
|                            | Potential for public concern | Elements of public expectation not being met | |
|                            |                                                                                  | National media coverage with <3 days service well below reasonable public expectation | |

| Business objectives/projects | Insignificant cost increase/schedule slippage | 5–10 per cent over project budget | Non-compliance with national 10–25 per cent over project budget |
|                            | Schedule slippage | Schedule slippage | Schedule slippage |
|                            |                                                              | Key objectives not met            | Key objectives not met |

|                                                                         |                                                                         |                                                                         |                                                                         |                                                                         |
|                                                                         |                                                                         |                                                                         |                                                                         |                                                                         |
|                                                                         |                                                                         |                                                                         |                                                                         |                                                                         |
A.1.2. Assess the likelihood of the risk crystallising

<table>
<thead>
<tr>
<th>Level</th>
<th>Detail description examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Rare</strong> – This will probably never happen / recur or may occur only in exceptional circumstances (up to 20%). The expected frequency is no more than once.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Unlikely</strong> – Do not expect it to happen / recur but it could occur at some time (21% to 40%).</td>
</tr>
<tr>
<td>3</td>
<td><strong>Possible</strong> – Might happen or recur at some time (41% to 60%)</td>
</tr>
<tr>
<td>4</td>
<td><strong>Likely</strong> - Will probably happen or occur in most circumstances (61% to 80%)</td>
</tr>
<tr>
<td>5</td>
<td><strong>Almost certain</strong> – Is expected to occur in most circumstances or recur, possibly frequently (81% to 100%)</td>
</tr>
</tbody>
</table>

A.2 Risk Prioritisation for Local Risks

All identified local or specialist risks affecting actions supporting Directorate Objectives will be rated in accordance with the following process:

A.2.1. Assess potential impact of risk on Directorate objectives and actions

The potential impact of local risks will be assessed using the same risk matrix as for corporate risks. However, the Finance domain scores have been adjusted to reflect the localised nature of the threat, as follows:

<table>
<thead>
<tr>
<th>Domains</th>
<th>Consequence score (severity levels) and examples of descriptors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Finance including claims</td>
<td>Negligible</td>
</tr>
<tr>
<td>Small loss less than 0.1 per cent of budget</td>
<td>Loss of 0.1–0.25 per cent of budget</td>
</tr>
<tr>
<td>Claim less than £100,000</td>
<td>Claim(s) between £100,000 and £250,000</td>
</tr>
<tr>
<td>Service/business interruption Environmental impact</td>
<td>Loss/interruption of &gt;1 hour</td>
</tr>
<tr>
<td>Minimal or no impact on the environment</td>
<td>Minor impact on environment</td>
</tr>
<tr>
<td></td>
<td>Major impact on environment</td>
</tr>
</tbody>
</table>
A.2.2. Assess the likelihood of the risk crystallising

<table>
<thead>
<tr>
<th>LIKELIHOOD OF RISK CRYSTALLISING (OCCURRING)</th>
<th>Detail description examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Rare – This will probably never happen / recur or may occur only in exceptional circumstances (up to 20%). The expected frequency is no more than once.</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely – Do not expect it to happen / recur but it could occur at some time (21% to 40%).</td>
</tr>
<tr>
<td>3</td>
<td>Possible – Might happen or recur at some time (41% to 60%)</td>
</tr>
<tr>
<td>4</td>
<td>Likely - Will probably happen or occur in most circumstances (61% to 80%)</td>
</tr>
<tr>
<td>5</td>
<td>Almost certain – Is expected to occur in most circumstances or recur, possibly frequently (81% to 100%)</td>
</tr>
</tbody>
</table>

A.2.3. Determine the overall risk rating by combining the potential impact of the risk and the likelihood of the risk crystallising

Any risk that scores 10 or above in the risk assessment process results in an overall risk rating of HIGH (Orange) and risks scoring over 20 are considered to be EXTREME (Red). Any risk scoring 9 or below in the risk assessment process results in an overall risk rating of MEDIUM (Yellow) and risks scoring below 4 results in an overall risk rating of LOW (Green).
# INFORMATION RISK POLICY

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER</th>
<th>CP57</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER</td>
<td>1</td>
</tr>
<tr>
<td>REPLACES SEPT DOCUMENT</td>
<td>CP57</td>
</tr>
<tr>
<td>REPLACES NEP DOCUMENT</td>
<td>N/A</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td>N/A</td>
</tr>
<tr>
<td>AUTHOR</td>
<td>Information Governance Manager</td>
</tr>
<tr>
<td>CONSULTATION GROUPS</td>
<td>IGSSC</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE</td>
<td>October 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S)</td>
<td>N/A</td>
</tr>
<tr>
<td>LAST REVIEW DATE</td>
<td>N/A</td>
</tr>
<tr>
<td>NEXT REVIEW DATE</td>
<td>January 2020</td>
</tr>
<tr>
<td>APPROVAL BY IGSSC</td>
<td>15th June 2018</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE</td>
<td>13th September 2018</td>
</tr>
</tbody>
</table>

## COPYRIGHT

© Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner.

## POLICY SUMMARY

This policy ensures that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation.

The Trust monitors the implementation of and compliance with this policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is

The Executive Chief Finance Officer
CONTENTS

1.0 INTRODUCTION
2.0 AIMS AND OBJECTIVES
3.0 SCOPE
4.0 RESPONSIBILITIES
5.0 DEFINITIONS
6.0 RISK MANAGEMENT STRUCTURE
7.0 TRAINING
8.0 IMPLEMENTATION
9.0 MONITORING
10.0 REFERENCE OTHER DOCUMENTS

APPENDICES

APPENDIX 1 – RISK PRIORITISATION SYSTEMS

APPENDIX 2 – INFORMATION GOVERNANCE RISK MANAGEMENT STRUCTURE
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION RISK POLICY

Assurance Statement
This policy ensures that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation.

1.0 INTRODUCTION

1.1 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Essex Partnership University NHS Foundation Trust (the ‘Trust’) continuously manages information risk.

1.2 The Board acknowledges that information risk management is an essential element of broader information governance / security and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not by imposing risk management as an extra requirement.

1.3 This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff, stakeholders and the Trust itself and therefore mechanisms to achieve and maintain appropriate protection of the Trust’s business critical information assets, will be developed through the maintenance of an Information Asset Register.

1.4 The risks associated with not complying with this policy include litigation, breach of law as well as loss of reputation to the Trust and potential impacts on service users.

2.0 AIMS AND OBJECTIVES

2.1 The Information Risk Policy will:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant ensuring information is held securely and used appropriately
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage pro-active rather than re-active information risk management
- Provide assistance to and improve the quality of decision making throughout the Trust
- Meet legal or statutory requirements
- Assist in safeguarding the Trust’s information assets
2.2 The following list provides some examples of where / how potential information risks can occur:

- Loss of data held on portable data storage devices (e.g. laptop, memory sticks, dictaphone tapes, iPhones, iPads, etc.)
- Incorrect use of passwords
- Incorrect use of smartcards
- Inappropriate access to personal information
- PC workstation security

The above list is not exhaustive.

3.0 SCOPE

3.1 This policy is to be made available to all Trust staff and observed by all members of staff, both clinical and administrative.

3.2 Information risk should be managed in a robust way within all work areas and should not be seen as the sole responsibility of the Information Governance Team.

3.3 This policy is applicable to all areas of the Trust and adherence should be included in all contracts for out-sourced or shared services. There are no exclusions.

4.0 RESPONSIBILITIES

4.1 The Chief Executive
The Chief Executive has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other major risks such as financial, legal and reputational risks.

4.2 Executive Chief Finance Officer and Senior Incident Risk Officer (SIRO)
The Executive Chief Finance Officer (SIRO) has overall responsibility and is familiar with and takes ownership for the implementation and management of the Trust’s information risk policy, with day to day management of the information risk management programme including information privacy and security and will provide assurances / advice to the Board of Directors in relation to information risk, governance and security through periodic reports and briefings.

4.3 Associate Director of System Implementation and Data Quality
The Associate Director of System Implementation and Data Quality will lead the Information Governance Team who will be responsible for the overall implementation and management of national and local guidance on information governance / security / risk, ensuring that processes and systems are established.
4.4 **Information Governance Manager**
The Information Governance Manager will oversee the day to day implementation of processes and systems in relation to information governance / security / risk coordinating the management of the Information Governance Toolkit and local / national guidance acting as a central point of contact / advice for both staff and external organisations.

4.5 **Information Asset Owners (IAOs)**
IAOs will be senior individuals (Deputy, Associate, Assistant Directors) whose role will be to understand and address risks to the identified information assets they 'own' and to provide assurances to the SIRO on the security and use of those assets through the process of implementation of information governance / security guidance.

4.6 **Information Asset Administrators (IAAs)**
IAAs will support the IAOs by ensuring that policies and procedures are followed, recognising actual or potential security incidents, consulting IAOs and the Information Governance Manager on incident management, and by ensuring that information asset registers are maintained accurate and up to date.

5.0 **DEFINITIONS**

5.1 Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of **consequence** and **likelihood** (see Appendix 1).

- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

- **Likelihood**
  A qualitative description or synonym for probability or frequency.

- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.

- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence
    - Reduce the consequences of occurrence
    - Transfer the risk
    - Retain/accept the risk

- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
6.0 POLICY REFERENCES / ASSOCIATED DOCUMENTATION

6.1 To build robust management of information risk the Trust will develop an information governance / security structure relying on the identification and ownership of information assets ensuring a structured approach to reporting and addressing risk.

6.2 The Trust’s information risk structure will be developed based on guidance from the Digital Information Policy team, NHS Connecting for Health: NHS Information Risk Management (January 2009), see Appendix 2.

7.0 TRAINING

7.1 To manage information risk effectively all staff will be required to undertake appropriate information governance / security training.

7.2 A staff training needs analysis will be undertaken in line with national guidance and requirements and a record of mandatory training will be kept.

7.3 Information governance / security training is mandatory and will be undertaken via the Trust’s OLM e-learning system.

For some specialist staff groups additional training will be required and identified within the Information Governance Toolkit Training Tool.

7.4 The Information Governance Toolkit sets out the compliance levels required and completion of the training modules is recorded and monitoring by information governance leads. Mapping reports will be monitored and sent to operational managers and directors identifying which of their staff are not compliant.

8.0 IMPLEMENTATION

8.1 The management of information risk is complex and the Trust has therefore developed a procedural guideline to support implementation of this policy. These guidelines are available via the Trust’s intranet site. They provide comprehensive information and guidance, where appropriate, that ensures all Trust staff are aware of their responsibilities in relation to the management of information / data.
9.0 MONITORING

9.1 The Executive Chief Finance Officer (SIRO) is responsible for monitoring the implementation and effectiveness of this policy and related procedural guidelines.

9.2 Monitoring of identified information risks and asset registers will be undertaken by the Trust’s Information Governance Steering Sub-Committee / Integrated Quality and Governance Steering Committee.

9.3 Information governance leads will provide the Board of Directors with ad hoc updates on any high level risks (red) which need escalating to the Board for further guidance to address those risks.

9.4 Implementation of this policy and its associated procedural guidelines will be undertaken as part of the overall Trust’s policy implementation audit programme.

10.0 REFERENCE OTHER DOCUMENTS

10.1 The following documents should be considered, read in conjunction with this policy and its procedural guidelines:

- Information Governance / Security policy / procedures
- Risk Management Framework
- Adverse Incident policy / procedures— including Serious Untoward Incidents procedures
- Records Management policy / procedures
- Data Protection & Confidentiality policy / procedures
- Checklist for reporting, managing and investigating Information Governance Serious Untoward Incidents (Gateway ref: 13177)
- Conduct and Capability policy / procedures
- Information Governance Toolkit (current version)

END
Other Relevant Acts of Parliament

1 Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS service users to respect and protect an individual’s human rights. This will include an individual’s right to privacy (under Article 8) and a service user’s right to expect confidentiality of their information at all times.

Article 8 of the Act provides that ‘everyone has the right to respect for his private and family life, his home and his correspondence’. However, this article also states ‘there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.

Each organisation must act in a way consistent with these requirements. It must take individuals rights into account when sharing personal information about them.

2 Freedom of Information Act 2000

This Act came into being in November 2000 and fully in force in January 2005. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities – this became effective in 2005. Further information will be available as implementation progresses (see www.ico.gov.uk).


This Act combines rules relating to access to protected electronic information as well as revising the ‘Interception of Communications Act 1985’. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

4 Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a
Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

5 **The Computer Misuse Act 1990**

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each user an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly and may be liable to criminal prosecution under the provisions of the Act.

6 **The Access to Health Records 1990**

This Act gives service user’s representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person’s records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

7 **Access to Medical Reports Act 1988**

This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

8 **Health & Social Care Act 2001: Section 60**

Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential service user information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This is intended primarily as a temporary measure until anonymisation measures or appropriate recording of consent can be put in place. Where the powers provided by this legislation are used to support the processing of confidential service user information there will be additional safeguards and restrictions on the use and disclosure of the information. These may differ from case to case and change over time where the process of annual review, required by the legislation, results in more stringent safeguards being applied.

---

*Health & Social Care Act 2008 - Reporting of infection to Public Health England or local authority and mandatory reporting of healthcare associated infection to Public Health England*
• This includes a requirement for NHS Trust Chief Executives to report all cases of MRSA, MSSA and \textit{E. coli} bacteraemias and \textit{Clostridium difficile} infection in patients aged two years or older that are identified in their institution.

\textit{Health Protection (Notification) Regulations 2010}

• These require attending doctors (registered medical practitioners) to notify the Proper Officer of the local authority of cases of specified infectious disease or of other infectious disease or contamination, which present, or could present, significant harm to human health, to allow prompt investigation and response. The regulations also require diagnostic laboratories testing human samples to notify Public Health England of the identification of specified causative agents of infectious disease.
### Glossary

<table>
<thead>
<tr>
<th><strong>Patient Identifiable Information</strong></th>
<th>Key identifiable information includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Patient’s name, address, full postcode, date of birth</td>
</tr>
<tr>
<td></td>
<td>- Pictures, photographs, videos, audio-tapes or other images (including digital)</td>
</tr>
<tr>
<td></td>
<td>- NHS Number and local patient identifiable codes</td>
</tr>
<tr>
<td></td>
<td>- Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analysis which identify small numbers within a small population may allow individuals to be identified.</td>
</tr>
</tbody>
</table>

| **Anonymised Information** | This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. |

| **Pseudonymised Information** | This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that data will only be identifiable to those that have the key or index. Pseudonymisation allows for information about the same individual to be linked in a way that true anonymisation does not. |

| **Clinical Audit** | The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish general knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research and is not encompassed within the definition of clinical audit in this document. |

| **Explicit/Express Consent** | This means articulated patient agreement. The terms are interchangeable and relate to clear and voluntary indication of preference or choice, given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear. |

<p>| <strong>Implied Consent</strong> | This means patients agreement that has been signalled by the behaviour of an informed patient. |</p>
<table>
<thead>
<tr>
<th><strong>Common Law Duty of Confidentiality</strong></th>
<th>This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that the information confided should not be used or disclosed further, except as originally understood by the confider, or without their subsequent permission.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disclosure</strong></td>
<td>This is the divulging or provision of access to data.</td>
</tr>
<tr>
<td><strong>Healthcare Purposes</strong></td>
<td>These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.</td>
</tr>
<tr>
<td><strong>Information Sharing Protocols</strong></td>
<td>Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security and confidentiality and data destruction, between two or more organisations or agencies.</td>
</tr>
<tr>
<td><strong>Medical Purposes</strong></td>
<td>As defined in the Data Protection Act 2018, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health &amp; Social care Act 2001 explicitly broadened the definition to include social care.</td>
</tr>
<tr>
<td><strong>Public Interest</strong></td>
<td>Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services.</td>
</tr>
<tr>
<td><strong>Social Care</strong></td>
<td>Social Care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes “pure” health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by other others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).</td>
</tr>
</tbody>
</table>
## DATA PROTECTION & CONFIDENTIALITY POLICY

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER:</th>
<th>CP59</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>2</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td>RE-draft for implementation of GDPR</td>
</tr>
<tr>
<td>AUTHOR:</td>
<td></td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>April 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td>March 2018</td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>March 2018</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>March 2020</td>
</tr>
<tr>
<td>APPROVAL BY IGSSC:</td>
<td>March 2018</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE:</td>
<td>May 2018</td>
</tr>
<tr>
<td>COPYRIGHT</td>
<td>© Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner</td>
</tr>
</tbody>
</table>

### POLICY SUMMARY

The purpose of this Policy is to ensure that staff understand their responsibilities regarding the General Data Protection Regulation (GDPR) & Data Protection Act (DPA) and the confidentiality of data, thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the “Trust”).

The Trust monitors the implementation of and compliance with this policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is

**Executive Chief Finance & Resources Officer**
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION & CONFIDENTIALITY POLICY

CONTENTS

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

1.0 INTRODUCTION
2.0 MANAGEMENT AND STAFF RESPONSIBILITIES
3.0 DEFINITIONS
4.0 REPORTING BREACHES
5.0 TRAINING AND SUPPORT
6.0 MONITORING AND REVIEW
7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION

APPENDICES

APPENDIX 1 – OTHER RELEVANT ACTS OF PARLIAMENT
APPENDIX 2 – GLOSSARY (TERMS USED WITHIN THE POLICY & PROCEDURE AND TERMS RELATED TO THE POLICY & PROCEDURE)
1.0 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) came into force on 25th May 2018. The new DPA 2018 is the UK legislation to come out of the GDPR; this enables the UK to stay in line with the EU as the original DPA1998 is considered no longer fit for purpose.

1.2 The GDPR is closely linked to the Freedom of Information and Human Rights Acts. Its focus is on promoting the rights of individuals in respect of their data, how it is used, stored and shared. Applies to ‘Data Controllers’ and ‘Data Processors’ - the controller says how and why personal data is processed.

1.3 The Trust has a legal obligation to comply with all appropriate legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the NHS Executive, other advisory groups to the NHS and guidance issued by professional bodies.

1.4 All legislation relevant to an individual’s right to confidentiality and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: service user administration, payment, purchasing, invoicing and treatment planning. Legislation also regulates the use of manual records relating to service users, staff and others whose information may be held within the Trust.

1.5 Patients expect that information about them will be treated as confidential and are given that assurance in the NHS Constitution for England, ‘You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure’ Patients who feel that confidence has been breached may issue a complaint under the NHS complaints procedure or they could take legal action.

1.6 The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised persons include NHS staff who are not involved in either the clinical care of the patient or the associated administration processes.
1.7 Non-compliance with the relevant legislation could result in individuals, employees and the Trust being prosecuted for offences under the GDPR. Article 5 GDPR requires that personal data shall be:

“a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Article 5(2) requires that:

“The controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

1.7.1 The risks associated with not complying with this policy and the associated procedures includes litigation, breach of law as well as loss of reputation to the Trust and potential impact on the service user.

2.0 MANAGEMENT AND STAFF RESPONSIBILITIES

2.1 The Chief Executive

2.1.1 The **Chief Executive** has overall responsibility for Data Protection and Confidentiality within the Trust.

2.2.2 The implementation of, and compliance with, these procedures and the associated policy is delegated to the Director of IT
2.2 The Data Protection Officer

2.2.1 The DPO’s minimum tasks are defined in Article 39:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed.

2.3 Service / Team / Ward Managers

2.3.1 The day-to-day responsibilities for enforcing these guidelines will lay with individual service managers and other nominated staff. In order to fulfill their roles, the Data Protection Officer will ensure that regular training is provided to remind designated staff of these responsibilities and the most effective way of ensuring adequate information security and confidentiality.

2.4 Individual Data Users

2.4.1 All employees of the Trust, who record and/or process personal data in any form (referred to as “Data Users”), must ensure that they comply with:

- The requirements of the GDPR & Data Protection Act (including the Data Protection Principles).
- The Trust’s data protection and confidentiality related policies, including any procedures and guidelines, which may be issued from time to time.

2.4.2 A breach of the GDPR, DPA and/or the Trust’s data protection and confidentiality related policies and procedures may result in disciplinary proceedings and may lead to an individual being personally liable for the breach.

2.4.3 Consideration should be given towards contacting the Data Protection Officer for data protection advice concerning the following:

- When developing a new computer system for processing personal data;
- When using an existing computer system to process personal data for a new purpose as it may be necessary to notify an amendment to an existing registration;
When creating a new manual filing system containing personal data;
When using an existing manual filing system containing personal data for a new purpose.

3.0 DEFINITIONS

3.1 “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;

3.2 “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.

3.3 Confidentiality (NHS Code of Practice)
3.3.1 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.

3.4 Personal Information:- (The GDPR applies to both automated personal data and to manual filing systems)

- Forename
- Surname
- Date of Birth
- Sex
- Address
- Postcode
- NHS Number, hospital number or other patient number
- Staff payroll number
- Bank details

(This list is not exhaustive...)
3.5 **Processing** includes (but is not limited to):

- Obtaining
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Use
- Transmission
- Erasure
- Destruction

(This list is not exhaustive...)

3.6 **A data subject** is an individual who is the subject of the personal data. A data subject must be a living individual.

3.7 **Data Controller**:-

- The individual, company or organisation who determines the purpose and the manner in which personal data may be processed.
- The Data Controller is EPUT

3.8 **Data Processor** in relation to personal data, means any other person other than an employee of the Data Controller who processes data on behalf of EPUT.

3.9 **Recipient**, in relation to personal data means any person to whom data is disclosed (including employees or agents of EPUT)

3.10 **Third Party**, means any person other than; the data subject, EPUT, any processor or other person authorised to process for EPUT

3.11 The **Information Asset Owner (IAO)** is the person or group of people who have been identified by management as having responsibility for the maintenance of the confidentiality, availability and integrity of that asset. The asset owner may change during the lifecycle of the asset.

3.12 The **Information Asset Administrator (IAA)** is the person or group of people who have been identified by the Information Asset Owner as having responsibility for adding information to the asset.

3.13 The IAO and nominated IAA will record their team assets on the Information Asset Management System (IAMS). This is a requirement with the NHS Digital Information Governance Toolkit. These assets are monitored and kept up to date. The Information Governance Team will advise and guide the nominated person from each team.
4.0 REPORTING BREACHES

4.1 Any potential or actual breaches of confidentiality must be reported to the line manager immediately.

4.2 The Information Governance Team should be notified and an incident report completed. The Information Governance Team will be able to give advice on how to rectify / reduce the impact of the breach.

4.3 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

(Note: refer to Information Security Incident Reporting Procedure (CPG50d))

5.0 TRAINING AND SUPPORT

5.1 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 Connecting for Health Information Governance website.
- Training via the Trust’s e-learning programme (OLM)
- 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 (HR21).

6.0 MONITORING AND REVIEW

6.1 The procedural guidelines will be reviewed in line with this policy document and / or whenever changes in legislation, guidance from Department of Health, the NHS Executive or the Information Commissioner’s Office require.
6.2 The Executive Medical Director is responsible as the Caldicott Guardian in association with the SIRO for the implementation of these procedural guidelines and its associated policy document.

7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION (Appendix 1)

7.1 Reference should be made to the following related documents:

- CPG59(b) – Confidentiality Procedure
- CPG59(a) – Data Protection Procedure
- CP / CPG53 – Whistle blowing Policy and Procedures
- CP / CPG25 – Freedom of Information Policy and Procedures
- CP / CPG50 – Information Governance and Security Policy and Procedures
- CP / CPG9 – Records Management Policy and Procedures
- CPG9(h) – Electronic Records (Laserfiche) Procedure
- CP61 – Paper and Electronic Corporate Records Procedure
- CP / CPG28 – Closed Circuit Television (CCTV) Policy
- CP60 / CPG60 – Information Sharing and Consent Policy and Procedures
- General Data Protection Regulation (2016)
- Data Protection Act 2018
- Police and Criminal Evidence Act 1984
- The Children’s Act 1989
- Human Rights Act 2000
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- The Computer Misuse Act 1990
- The Access to Health Records Act 1990
- Access to Medical Records Act 1988
- Health and Social Care Act 2001 (Section 60)
- NHS Code of Practice: Confidentiality (Dept of Health Guidance)
- HSC 1990/012: Caldicott Guardians (Established the role of the Caldicott Guardian within Health Service organisations)
- HSC 2002/012: Caldicott Guardians & Implementing the Caldicott Standards into Social Care (Provides guidelines relating to sharing of service user identifiable information)
- HSC 1999/053: For the Record (Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as service users, employees, volunteers etc.)
- ISO/IEC 27000 Series – Information Security Standards (This is the accepted industry standard for information management and security)
- Health and Social Care Act 2012/2015

(This list is not exhaustive)
8.0 APPENDICES

8.1 Appendix 1 – Other relevant Acts of Parliament

8.2 Appendix 2 – Glossary (terms used within the policy & procedure and terms related to the policy & procedure)

END
PAPER AND ELECTRONIC CORPORATE RECORDS POLICY

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER:</th>
<th>CP61</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>5</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td>Reviewed and updated details</td>
</tr>
<tr>
<td>AUTHOR:</td>
<td>Records Manager</td>
</tr>
<tr>
<td>CONSULTATION GROUPS:</td>
<td>Information Governance Steering Committee</td>
</tr>
<tr>
<td></td>
<td>Quality Committee</td>
</tr>
<tr>
<td></td>
<td>Paris Project Board</td>
</tr>
<tr>
<td></td>
<td>Mobius Project Board</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>April 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td>November 2018 (GDPR), March 2019</td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>June 2019</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>Aug 2022</td>
</tr>
<tr>
<td>APPROVAL BY INFORMATION GOVERNANCE STEERING COMMITTEE:</td>
<td>March 2019</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE:</td>
<td>June 2019</td>
</tr>
<tr>
<td>COPYRIGHT</td>
<td>© EPUT 2018</td>
</tr>
</tbody>
</table>

Policy Summary:

The purpose of this Policy Guideline document is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of paper and electronic corporate records.

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

This process is monitored via the Data Security & Protection Toolkit and assurance reports are submitted to the Information Governance Steering Committee.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>![ ]</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
Executive Chief Finance Officer
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 INTRODUCTION</td>
</tr>
<tr>
<td>2.0 SCOPE</td>
</tr>
<tr>
<td>3.0 PURPOSE</td>
</tr>
<tr>
<td>4.0 RESPONSIBILITIES</td>
</tr>
<tr>
<td>5.0 DEFINITIONS</td>
</tr>
<tr>
<td>6.0 LEGAL AND PROFESSIONAL OBLIGATIONS</td>
</tr>
<tr>
<td>7.0 IMPLEMENTATION</td>
</tr>
<tr>
<td>8.0 MONITORING COMPLIANCE</td>
</tr>
<tr>
<td>9.0 REFERENCE TO OTHER POLICIES AND PROCEDURES</td>
</tr>
</tbody>
</table>
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PAPER AND ELECTRONIC CORPORATE RECORDS POLICY

Assurance Statement

The purpose of this policy is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of paper and electronic corporate records. This policy has been developed in accordance to the Information Governance Alliance – Records Management Code of Practice 2016, and other relevant guidance and legislation and general good practice in records management.

1.0 INTRODUCTION

1.1 Records management is the process by which an organisation manages all the aspects of its records, whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal or transfer to National Archives / County Archives.

1.2 The Information Governance Alliance have published an NHS Records Management Code of Practice 2016; this document has been put together as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

1.3 The Trust’s records (as defined below) are its corporate memory, providing evidence of actions and decisions; they represent a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of service users, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.4 This document sets out a framework within which the staff responsible for managing the organisation’s records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.5 The key consideration of this policy is the way that records are created and filed. Filing systems are at the heart of information storage and retrieval activities. They will ensure that records are accessible and retrievable when and where required, to meet business needs and information access requests (such as Freedom of Information), whilst protecting their security and integrity.

1.6 The Trust has invested in a corporate Electronic Document and Records Management (EDRM) system from Laserfiche. This will be used for filing all corporate electronic records at a suitable point in their lifecycle. It provides capabilities for storage and retrieval, version control, retention and disposal.
2.0 SCOPE

2.1 In the context of Corporate Information Assurance, corporate information refers to information generated by an organisation other than clinical/care (or service user) information. It will therefore include records from the following (and other) areas of the Trust:

- Estates/Engineering
- Financial
- Information Management & Technology (IM&T)
- Personnel/Human Resources
- Purchasing/Supplies

This list is not exhaustive....

3.0 PURPOSE

3.1 The purpose for a Records Management system is to ensure that:

- **Records are available whenever needed or requested**, The Trust is able to form an audit of the activities or events that have taken place.
- **Records can be accessed**, both records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.
- **Records can be interpreted**: the context of the record can be interpreted: who created or added to the record and when, during which business process it was created / amended, and how the record is related to other records.
- **Records can be trusted**, the record reliably represents the information, and that its integrity and authenticity can be demonstrated.
- **Records can be maintained through time**, the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.
- **Records are secure**, from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.
- **Records are retained and disposed of appropriately**, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.
- **All Staff are appropriately trained**, so that they are made aware of their responsibilities for record-keeping and record management.
4.0 RESPONSIBILITY

4.1 Chief Executive

4.1.1 The Chief Executive has overall responsibility for records management within the Trust, as accountable officer, and is responsible for the management of the Trust and for ensuring that appropriate mechanisms are in place to support the service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

4.2 Director of ITT

4.2.1 The Director of ITT has delegated responsibility for ensuring appropriate measures are developed and implemented and that adequate procedures and good practice are in place and followed and enforced to ensure good records management underpins the work of the Trust.

4.2.2 This delegated responsibility includes:

- The development of Electronic Management Systems for electronic records;
- Developing action plans to address records management issues arising from Risk Management Standards (RMS), Information Governance and other reviews.
- Ensuring appropriate training in records management is provided.

4.3 Data Protection Officer (Legal Services Manager)

4.3.1 The Data Protection Officer is responsible for the development, implementation, compliance, monitoring and review of the data protection legislation, including providing guidance on corporate records management issues, and ensuring that related policies and procedures conform to the latest legislation and NHS guides on data protection, confidentiality, information security and rights of access to information (Subject Access Requests).

4.4 Freedom of Information / Environmental Information Regulations Team (Legal Team)

4.4.1 The Legal Team will provide advice and support on the Freedom of Information Act and the Environmental Regulations Act.

4.5 Individual Responsibilities

4.5.1 All staff, whether clinical or administrative, who create, receive and use corporate records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and any subsequent guidance issued.
5.0 DEFINITIONS

Definition of a Record:-

5.1 Records are defined as ‘recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity’.

5.2 These can be primary, management or support activities. They are kept as audit trail evidence of and information about the Trust’s functions, decisions, processes, procedures, operations, proper conduct, rights and obligations, transactions or other activities of the organisation.

5.3 Records can exist in any medium and format, both electronic and hard copy, including but not restricted to e-mail messages, word processing and spreadsheet documents, presentations, PDFs, desktop publishing, scanned images, instant messages, audio, video, databases, electronic forms, computer reports, photographs, CAD and maps.

Definition of Information:-

5.4 This is a corporate asset. The Trust’s records are important sources of administrative, evidential and historical information. They are vital to the organisation to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purposes of accountability, and for an understanding of its history and procedures.

Definition of a Records Lifecycle:-

5.5 This describes the life of a record from its creation / receipt into the organisation, through the period of its “active” use, then into a period of “inactive” retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

Definition of Records Management:-

5.6 This is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is legally sound, serves the operational needs of the organisation and preserves an appropriate historical record. The key components are:-

- Record Creation
- Record Keeping
- Record Maintenance (including tracking of record movements)
- Access and Disclosure
- Closure and Transfer
- Appraisal
- Archiving
- Appropriate Disposal
6.0 LEGAL AND PROFESSIONAL OBLIGATIONS

6.1 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Information Governance Alliance Code of Practice - Records Management in particular:

- The Public Records Act 1958
- The Data Protection Act 2018
- General Data Protection Regulation 2016
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Any new legislation affecting records management as it arises.

7.0 IMPLEMENTATION

7.1 The management of records is a complex process with the need to comply with much guidance and legislation. The Trust has therefore developed a range of procedural guidelines to support implementation of this policy. These guidelines are available on the Trust's intranet site. They provide comprehensive information and guidance, where appropriate, that ensures all Trust staff are aware of their responsibilities for records from creation, through day-to-day use, selection, storage, maintenance and finally disposal/archive.

8.0 MONITORING COMPLIANCE

8.1 The Executive Chief Finance Officer is responsible for monitoring the implementation and effectiveness of this policy and related procedural guidelines.

9.0. REFERENCE TO OTHER POLICIES AND PROCEDURES

9.1 When processing records in any capacity reference should be made to any Trust policies relating to records as well as to local and professional guidance.

9.2 Other documentation will include:

- Records Management Policy / Procedures
- Data Protection and Confidentiality Policy / Procedure
- Information Governance and Security Policy / Procedures
- Information Sharing and Consent Policy / Procedure
- Records Management Lifecycle Strategy
- Freedom of Information Policy / Procedure

This list is not exhaustive….

END
INFORMATION GOVERNANCE & SECURITY
PROCEDURE

PROCEDURE NUMBER: CPG50
VERSION NUMBER: 2

KEY CHANGES FROM PREVIOUS VERSION
GDPR

AUTHOR: Information Governance Team
CONSULTATION GROUPS: IGSSC
IMPLEMENTATION DATE: April 2017
AMENDMENT DATE(S): July 2018
LAST REVIEW DATE: July 2018
NEXT REVIEW DATE: July 2021
APPROVAL BY: IGSSC September 2018
RATIFIED BY: TBC

COPYRIGHT © Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner.

POLICY 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 policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
The Executive Chief Finance Officer
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 INTRODUCTION</td>
</tr>
<tr>
<td>2.0 GENERAL INFORMATION</td>
</tr>
<tr>
<td>3.0 IMPLEMENTATION AND MANAGEMENT</td>
</tr>
<tr>
<td>4.0 RISK</td>
</tr>
<tr>
<td>5.0 TRAINING</td>
</tr>
<tr>
<td>6.0 MONITORING, REVIEW AND PERFORMANCE MANAGEMENT</td>
</tr>
<tr>
<td>7.0 REFERENCE TO OTHER DOCUMENTATION / LEGISLATION</td>
</tr>
</tbody>
</table>
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 Data Protection Act, 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 Information Governance 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.

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 / 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)
- Computer Misuse Act (1990)
- Electronic Communications Act (2000)
- The Re-Use of Public Sector Information Regulations (2005)
- The Civil Contingencies Act (2004)
- The Copyright, Designs and Patents Act (1988) (as amended by the Copyright Computer Programs Regulations (1992))
- The Health and Safety at Work Act (1974)
- Crime and Disorder Act (1998)
- The Common Law Duty of Confidentiality
- General Data Protection Regulation

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

END
<table>
<thead>
<tr>
<th>SECURITY / CONFIDENTIALITY BREACH</th>
<th>INCIDENT NO……….. (to be completed by the Information Governance Department)</th>
</tr>
</thead>
</table>

**Department:** .................................................................

**Directorate:** .................................................................

**Location/Site:** .................................................................

**Reporting Officer(s):** ......................................................

**Telephone Number:** ...........................................................

**Incident Reported to:** .......................................................

**Date Reported:** .................................................................

**Incident Date:** .................................................................

*(if known, else approximate)*

**Incident Description:**


INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE - CPG50(D)
(September 2016)

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:
## CLASSIFICATION OF INFORMATION GOVERNANCE / SECURITY INCIDENTS

<table>
<thead>
<tr>
<th>CONSEQUENCE</th>
<th>TYPE OF EFFECT</th>
<th>Departmental Embarrassment</th>
<th>Personal Safety</th>
<th>Personal Privacy Infringement</th>
<th>Failure to Meet Legal Obligation</th>
<th>Commercial Confidentiality Loss</th>
<th>Financial Loss</th>
<th>Disruption to Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Contained within Department or Division</td>
<td>Minor injury to individual</td>
<td>Isolated personal detail revealed</td>
<td>Civil suit. &lt;£10k damages</td>
<td>Up to £10K</td>
<td>Up to £10K</td>
<td>Up to £10K</td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Contained within the Trust</td>
<td>Minor injury to several people</td>
<td>Isolated personal detail compromised</td>
<td>Civil suit &lt;£10K Small fine, &lt;£1K</td>
<td>£10K to £100K</td>
<td>£10K to £100K</td>
<td>£10K to £100K</td>
<td></td>
</tr>
<tr>
<td>Significant</td>
<td>Local public or press interested PQ raised</td>
<td>Major injury to individual</td>
<td>Several personal details revealed</td>
<td>Large fine (above £10K)</td>
<td>£100K to £500K</td>
<td>£100K to £500K</td>
<td>£100K to £500K</td>
<td></td>
</tr>
<tr>
<td>Major</td>
<td>National public or press aware — NAW or Commons debate</td>
<td>Major injury to several people. Death of individual</td>
<td>Several personal details compromised</td>
<td>Custodial sentence imposed</td>
<td>£500K to £1 million</td>
<td>£500K to £1 million</td>
<td>£500K to £1 million</td>
<td></td>
</tr>
<tr>
<td>Catastrophic</td>
<td>Minister forced to resign. No confidence motion against Government</td>
<td>Death of Several people</td>
<td>All personal details revealed and/or compromised</td>
<td>Multiple civil or criminal suits</td>
<td>Above £1 million</td>
<td>Above £1 million</td>
<td>Above £1 million</td>
<td></td>
</tr>
</tbody>
</table>
**INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE - CPG50(D)**

(March 2016)

**RISK MATRIX** from Connecting for Health Guidance Digital Information Policy guidance – Checklist for Reporting, Managing and Investigating Information Governance Serious or Untoward Incidents (January 2009).

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>No significant reflection on any individual or body</td>
<td>Damage to an individual's reputation. Possible media interest, e.g., celebrity involved</td>
<td>Damage to a team's reputation. Some local media interest that may not go public</td>
<td>Damage to a service's reputation/Local media coverage.</td>
<td>Damage to an organisation's reputation/Local media coverage.</td>
<td>Damage to NHS reputation/National media coverage.</td>
<td></td>
</tr>
<tr>
<td>Media interest very unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor breach of confidentiality. Only a single individual affected</td>
<td>Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted</td>
<td>Serious potential breach &amp; risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected</td>
<td>Serious breach of confidentiality e.g. up to 100 people affected</td>
<td>Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected</td>
<td>Serious breach with potential for ID theft or over 1000 people affected</td>
<td></td>
</tr>
</tbody>
</table>
INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

<table>
<thead>
<tr>
<th>PROCEDURE NUMBER:</th>
<th>CPG50D</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>6</td>
</tr>
<tr>
<td>REPLACES SEPT DOCUMENT:</td>
<td></td>
</tr>
<tr>
<td>REPLACES NEP DOCUMENT:</td>
<td></td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION:</td>
<td></td>
</tr>
<tr>
<td>AUTHOR:</td>
<td>Information Governance Team</td>
</tr>
<tr>
<td>CONSULTATION:</td>
<td>Information Governance Steering Sub-Committee;</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>April 2017</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td>November 2011, April 2013, May 2014 (Director Change), March 2016</td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>July 2018</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>July 2021</td>
</tr>
<tr>
<td>APPROVAL BY INFORMATION GOVERNANCE &amp; SECURITY SUB-COMMITTEE:</td>
<td>September 2018</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE:</td>
<td>TBC</td>
</tr>
<tr>
<td>COPYRIGHT:</td>
<td>© Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner</td>
</tr>
</tbody>
</table>

POLICY 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, and 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 policy 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. Incidents will be managed through the Trust Datix System.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is

The Executive Chief Finance Officer
INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONTENTS

1.0 INTRODUCTION
2.0 RESPONSIBILITIES
3.0 REPORTING PROCEDURES

APPENDICES

APPENDIX 1 – SECURITY INCIDENT OPENING REPORT FORM
APPENDIX 2 – INFORMATION SECURITY INCIDENT INVESTIGATION FORM
APPENDIX 3 – CLASSIFICATION OF INFORMATION GOVERNANCE / SECURITY INCIDENTS
This procedure aims to ensure that all Trust staff are aware of the procedures that need to be followed in the event of an information security incident / information confidentiality breach and that risk of disruption to the Trust’s operations are minimised.

This procedure is linked to the Adverse Incident Policy and Procedures and should therefore be read in conjunction with CP3 & CPG3.

1.0 INTRODUCTION

1.1 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.

2.0 RESPONSIBILITIES

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

2.2 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.

2.3 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.

2.4 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.

3.0 REPORTING PROCEDURES

3.1 Overview

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

3.1.2 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.

3.1.3 All incidents whether they are actual or near misses must reported by staff within 48 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.

3.1.4 The Information Governance Team will categorise the incident / breach within one of the classifications (from insignificant to acute) as defined in the NHS Executive’s Incident Classifications Table.
3.1.5 The Information Governance Team will report all Level 2 incidents / breaches to the ICO. 

3.1.5 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.

3.1.7 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.

3.2 Reporting Procedures if Datix is available for use.

3.2.1 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.

3.2.2 **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.

3.2.3 **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.

3.2.4 **Area:**

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

3.2.5 **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.
3.2.6 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).

3.2.7 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)

3.2.8 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)

3.3 Reporting Procedures if Datix is not available for use.

3.3.1 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.

3.3.2 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).

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

3.3.4 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.

3.3.5 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.

3.3.6 Where the incident / breach impacts on the Trust’s computer, network, server delivery the Information Governance Manager 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.

3.3.7 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.

3.3.8 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.

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

END
PROCEDURE SUMMARY

These procedures and their associated policy document will ensure that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation (2016).

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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this procedure is

Executive Chief Finance Officer
CONTENTS

1.0 INTRODUCTION

2.0 INFORMATION RISK

3.0 RESPONSIBILITIES

4.0 MANAGING INFORMATION RISK

5.0 REPORTING

6.0 TRAINING

7.0 MONITORING AND AUDIT
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

INFORMATION RISK PROCEDURE

Assurance Statement

These procedures and their associated policy document will ensure that Essex Partnership University NHS Foundation Trust is compliant with its obligations to protect the Trust, its staff, patients, stakeholders and the wider general public from information risks and is compliant with its obligations under the General Data Protection Regulation (2016).

1.0 INTRODUCTION

1.1 Information used by the Trust is an important business asset in terms of both 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 staff that the Trust holds and manages.

1.2 Information risk is inherent in all administrative and business activities and it is vital that confidentiality, integrity and availability of information is maintained and that everyone working for or on behalf of the Essex University NHS Foundation Trust (the ‘Trust’) understands and continuously manages information risk.

1.3 These procedural guidelines will underline the way in which the Trust manages personal and sensitive information / data and the risks associated with this activity ensuring that such information is dealt with in line with legislation, securely, efficiently and effectively and thus preserving the Trust’s reputation.

1.4 The Trust places increasing reliance on technology, computers and, to an extent, third party contractors, to store and manage its information, and with the 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 same held, both in electronic and manual systems.

1.5 The Board of Directors recognises that the aim of information risk management is not necessarily being able to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.
2.0 INFORMATION RISK

2.1 The key to managing information risk is to identify, risk assess and monitor information assets across the organisation ensuring any breaches of confidential information / data / assets are reported in accordance with Trust policy.

2.2 Information assets come in many shapes and forms and it is generally best to group information assets in a logical manner and the Trust will manage its information assets by Directorate.

2.3 Information assets include, but are not restricted to:

| Personal Information Content | Databases; data files; back-up data; archive data; audit data; paper records (patient case notes / staff records); paper reports |
| Other Information Content | Databases; data files, audit data; paper records; paper reports |
| System / Process Documentation | System information and documentation; operations and support procedures; manuals and training materials; contracts and agreements; business continuity plans |
| Software | Applications and system software; data encryption utilities; development and maintenance tools |
| Hardware | Computing hardware including: PCs, laptops, PDA, communication devices, e.g. Blackberries and removable media, iPhones, iPads, etc. |
| Miscellaneous | Environmental services, e.g. power and air conditioning; people skills and experience; shared service (including networks and printers); computer rooms and equipment; records libraries |

3.0 RESPONSIBILITIES

3.1 SIRO (Senior Information Risk Owner)
3.1.1 The SIRO will have responsibility for the management of information risks, ensuring regular reporting mechanisms are established (quarterly) with Information Asset Owners / Administrators (IAOs / IAAs) and the Information Governance Manager to monitor those risks through the medium of the Information Governance Group.
3.1.2 The Information Governance Manager will provide ad hoc reports to the Quality Committee and the Information Governance Steering Sub-Committee advising of the processes / systems put in place to manage identified risk.

3.2 IAOs / IAAs
3.2.1 Electronic registers of the Trust’s information assets will be held by the IAOs / IAAs of the relevant Directorate with an overall register held by the Information Governance Manager.

3.2.2 IAOs / IAAs will be responsible for ensuring a review of information data flows and asset registers and undertaking risk assessments to identify any information risks.

3.2.3 IAOs / IAAs will provide the SIRO with a regular written report, quarterly, advising of any new information risk and updating on actions identified to address known risks.

3.3 Information Governance Manager
The Trust’s Information Governance Manager will initiate and continually update and review a process for recording information flows which in turn will assist in the identification of information assets.

Information risks and associated action plans to reduce or eliminate the risk will be monitored by the Information Governance Steering Sub-Committee / Quality Committee.

Information risks will be risk assessed in line with the Trust’s overall Risk Management Strategy.

3.4 Data Protection Officer
The DPO has the expert knowledge of data protection law and practices and detailed understanding of the organisation’s business, the purposes for which it processes, or intends to process personal data.

The DPO facilitates ‘accountability’ and the organisation’s ability to demonstrate compliance with the GDPR.

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.

The Data Protection Officer will take responsibility for providing expert advice and the promotion of data protection compliance and best practice.

3.5 All Staff
All staff will be responsible for managing the risk associated with the information / data that they handle and for ensuring that any identified risks are escalated through line management.
4.1 Data Flow Mapping

In order to assess where information risks may come from the Trust will undertake regular data flow mapping exercises and updates. Data flow mapping supports the development of Asset Registers and ensures the Trust is aware of any risk areas. This work will be undertaken on an individual basis and in line with national guidance (the most current version of the Information Governance Toolkit).

4.2 Asset Registers

Asset Registers are a recorded document of the Trust’s information assets and include detail of, e.g. databases, data files, systems, manuals, etc. See 4.3 above.

The development of the Trust’s information asset register will fall out of the data flow mapping exercises with registers being reviewed and amended in line with updates to data flow mapping.

Information assets, amendments, reviews updates and management of identified risks will be the responsibility of the Information Asset Owners supported by, where appropriate, Information Asset Administrators.

4.3 Information Risks

Risks to information / data / assets will be identified through a variety of measures, for example from:

- data flow mapping
- management of Asset Registers
- information governance / security awareness programmes
- Incidents and lessons learned from incidents

Identified risks will be risk rated according to the Trust’s risk management strategy and associated risk rating matrix and escalated as appropriate via the most appropriate committee / group (Information Governance Sub-Committee, Trust Records Group, Clinical Governance Committee / Quality Committee).

Any high risk areas will be escalated through to the Trust’s Executive Team / Board of Directors for further advice and guidance.

4.4 Incident Reporting

The reporting of information / data breaches will be undertaken in line with the Records Management, Information Governance / Security and Adverse Incident procedures.
5.0 REPORTING

5.1 Regular reports on data flow mapping, asset registers and the management of information risks will be provided to the SIRO and / or appropriate groups / committees.

5.2 Ad hoc reports will be provided to the Executive Team / Board of Directors when required to advise of newly identified risk, updates to known risks.

6.0 TRAINING

6.1 Training required to manage information risks will fall out of information governance / security training programmes and where appropriate, will be facilitated by the information governance leads (e.g. data flow mapping, asset registers).

7.0 MONITORING AND AUDIT

7.1 Monitoring will take place through internal and external audit of information governance / security processes and the Information Governance Toolkit.

END
**Transfers of Information outside the UK**  When can personal data be transferred outside the European Union?

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals’ rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

The EEA is made up of the 28 EU Member States, which are currently:

Austria Belgium Bulgaria Cyprus
Czech Republic Croatia
Denmark Estonia Finland France Germany
Greece Hungary Ireland Italy Latvia
Lithuania Luxembourg Malta Netherlands Poland
Portugal Romania Slovakia Slovenia Spain
Sweden United Kingdom (Exit in process)

**Plus** Iceland, Liechtenstein and Norway

Countries outside the EEA, known as *third countries*, currently deemed to have an adequate level of protection for personal data are,

Argentina Canada Guernsey Switzerland Isle of Man

As of yet, the United States does not have any centralized, formal legislation at the federal level regarding this issue, but does insure the privacy and protection of data through the United States Privacy Act, the Safe Harbor Act and the Health Insurance Portability and Accountability Act
**Department of Health guidelines**

In the case of person-identifiable data, regard must be paid to the guidelines issued by the Department of Health. The requires that such information is *NOT* transferred outside of the UK unless appropriate assessment of risk has been undertaken and mitigating controls put in place.

*Important:* The Trust must also consider the other Data Protection Principles before making an overseas transfer of person-identifiable data.
Keeping Confidential Information Secure

Good Practice

Confidential information must:

- **Not** be shared or discussed with, or in the presence of, anyone who does not need to know, or is not specifically authorised to know that information.

- Have appropriate control applied, having regard to professional ethics and patient consent. Applying formal access controls for clinical records and statutory requirements.

- Have appropriate control applied over the disclosure on non-patient information e.g. staff, relative, visitors in accordance with statutory requirements.

- **Not** be shared with parties outside the NHS e.g. solicitors, insurance companies, employers, police without the written consent of the individual concerned unless there are specific powers to do so.

- Always be stored in a secure location, preferably a room that is locked and in some cases alarmed when unattended.

- Not to be taken home or removed from the Trust without specific authorisation, this specifically applies to patient’s health records or patient data.

For all types of records, staff working in areas where personal records may be seen must:

- Shut/lock doors and cabinets as required.
- Adopt a “clear desk” policy where possible.
- Wear Trust identification badges or other authorised identification
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- **Not** tell unauthorised personnel how the security systems operate.
- **Not** breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the
transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored securely when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage – with permitted access. The availability of a secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have a need to access records, then appropriate access should be organised for them – this must not be by using others’ access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords (use 6-8 characters), or using names or words that are known to be personally associated with them (e.g. children’s or pet names or birthdays).
- Always clear the screen of a previous patient’s information before seeing another.
- Use a password-protected screen-saver where possible to prevent casual viewing of patient information by others.
- Protect information from the view of others as far as possible, particular care when there is a visitor present.
- Ensure that unwanted confidential printouts are shredded using a cross cutting shredder where possible and disposed of in confidential waste bins and in accordance with Trust policy on record disposal.
- Ensure that electronic media such as CD and Computer hard drives are disposed of in accordance with IT policy and procedures.

Telephone enquiries should be validated by:

- Checking the identity of the caller.
- Checking whether they are entitled to the information they request.
- Taking the calling number, verifying it independently and calling back if necessary.

Staff should ensure that general conversation involving discussions about individuals (including telephone) is:

- Where appropriate, undertaken in an area out of earshot of others, preferably in a
closed office.

- **Not** undertaken with anyone who is not authorised to receive the information, including family and friends.
- Restricted to the use of personal identifiers (e.g. hospital number) when in public/reception areas

**Confidential information sent via internal post or in internal transit should always be:**

- Appropriately addressed to a named recipient, post holder, consultant or legitimate Safe Haven (Trust nominated secure area).
- Sealed in an appropriately secure envelope/package based on sensitivity and volume
- Marked accordingly, with “Confidential” or “Addressee Only” as appropriate.
- Traced in or out and signed for as appropriate.

**Confidential information sent via external post or in external transit should always:**

- Be addressed fully and marked accordingly, with “Confidential” or “Addressee Only” as appropriate.
- Be sealed in an appropriately secure envelope/package based on sensitivity and volume and using tamper proof seals where practicable and appropriate.
- Be sent via an approved carrier such as NHS courier, Internal transport or recorded delivery for any confidential information sent in quantity such as patient health records or a collection of patient information on paper or printout, CD or other media. Obtaining a receipt as proof of sending/delivery is advised where possible.
- Traced in or out and signed for as appropriate.
- Have appropriate authorisation for leaving the Trust particularly in the case of patient’s health records.

**Staff wishing to send or receive confidential patient information via fax must:**

- Adhere to the Trust Safe Haven Procedures.
- Only send personal identifiable data to a recognised NHS Safe Haven (nominate secure area) fax number.
- Remove all identifiable data if not sending to a recognised NHS Safe Haven number
- Address the fax to a named recipient.
- Always check the number to avoid misdialling, check the number is correct and current if stored in a fax memory prior to sending.
- Ensure that trust fax machines are placed in secure locations, preferably within the boundary of a Safe Havens (Trust nominated secure area). As a minimum fax machines should be locked when unattended, switched off outside normal working hours or safely secured in lock cupboards if left switched on.
Staff using E-Mail must: (refer: Internet/Email Access and Use Procedural Guidelines (CPG50(B))

- Not e-mail person identifiable information externally to the Trust unless standard encryption software has been implemented and approved by the IT department. NHS mail is the approved method for transferring person identifiable information; otherwise, password protection and encryption are advised. Only e-mail person identifiable information when the Caldicott Principles are applied (anonymised where possible) and by placing the identifiable information in a password protected attachment and not including person identifiable information in the subject line or body of the email.
- Check to ensure that the recipient is authorised to receive the data (be careful of shared mailboxes).
- Ensure that extra care is taken to ensure that it is sent to the correct person (use of personal address books is recommended).

Staff working offsite:
(In relation to confidential data (inc. patient, staff, corporate, full or part records)
- Staff who have a need to carry paper records offsite should work in line with the Trusts’ Transportation (CPG9f) and Data Protection (CPG59) Procedures.
- Should only carry paper data if electronic alternatives are unavailable
- Should seek advice from Line Managers / Information Governance Team if in doubt.
- All items should be transported in locked boot of car and removed and taken with the staff member on arrival.
DATA PROTECTION PROCEDURE

POLICY REFERENCE NUMBER: CPG59a
VERSION NUMBER: 2
KEY CHANGES FROM PREVIOUS VERSION: Made compliant with GDPR
AUTHOR: [Redacted]
CONSULTATION GROUPS: IGSSC
IMPLEMENTATION DATE: MAY 2018
AMENDMENT DATE(S): March 2018
LAST REVIEW DATE: N/A
NEXT REVIEW DATE: November 2019
APPROVAL BY IGSSC: MARCH 2018
RATIFICATION BY QUALITY COMMITTEE: © Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

POLICY SUMMARY

The purpose of this Procedure is to ensure that staff understand their responsibilities regarding the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA"), thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the "Trust").

The Trust monitors the implementation of and compliance with this policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is
Executive Chief Finance Officer
DATA PROTECTION PROCEDURE – CPG59a

CONTENTS

1.0 INTRODUCTION
2.0 DATA PROTECTION PRINCIPLES
3.0 EXEMPTIONS
4.0 RETENTION OF INFORMATION
5.0 REPORTING BREACHES
6.0 TRAINING AND SUPPORT
7.0 MONITORING AND REVIEW

APPENDICES

APPENDIX 1 – TRANSFER OF INFORMATION OUTSIDE THE UK

APPENDIX 2 – KEEPING CONFIDENTIAL INFORMATION SECURE (GOOD PRACTICE)
DATA PROTECTION PROCEDURE

1.0 INTRODUCTION

1.1 The General Data Protection Regulation (GDPR) defines data as any information which:

- is processed using equipment operating automatically in response to instructions,
- is recorded with the intention of being processed,
- is recorded as part of a relevant filing system,
- forms part of an accessible record, including health records.

1.2 Data Protection is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual.

1.3 Personal data, within the Trust, is taken to include:

- all identifiable person information, including health records,
- all identifiable staff information,
- any other identifiable personal information held on suppliers, contractors etc.

(Note: Whether held in electronic or paper form)

1.4 Certain types of data are regarded as sensitive, and the GDPR Article 9 stipulates that special measures must be taken in the processing and protection of this type of data. “Special categories of personal data” (Sensitive) data includes:

- racial and ethnic origins,
- political opinions,
- religious other similar beliefs,
- membership to a trade union,
- physical or mental health or conditions,
- sexual life,
- processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- the commission of any offence, or
- any proceedings for any offence, or the sentence of any court in such proceedings.

1.5 The Trust collects and uses information about identifiable individuals in the course of its operations. This includes current, past and prospective patients, employees, suppliers, contractor clients / customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect
and use certain types of personal information to comply with the requirements of government departments. Under the GDPR, all forms of personal information must be dealt with properly however it is collected, recorded and used – whether automatically, within accessible records or relevant filing systems – and there are safeguards to ensure compliance.

1.6 All staff employed by the Trust are affected by the GDPR

- they have rights as employees about whom data is held, and
- they have obligations as health care professionals who collect data about patients and clients.

2.0 DATA PROTECTION PRINCIPLES

2.1 The aims of this procedure are to deliver fully the Principles of Data Protection, as stated in the GDPR Article 5.

The Principles require that:

2.2 a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest; scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal which is inaccurate –having regard for the purpose they are processed for – are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights & freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Article 5(2) requires that: “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

2.3 The Trust has to ensure that all information held on any media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

2.3.1 A definition of data quality is a measure of the degree of usefulness of the data for a specific purpose. Data needs to be:

- **Complete** (in terms of having been captured in full)
- **Accurate** (the proximity of the figures to the exact or true values)
- **Relevant** (the degree to which the data meets current and potential user’s needs)
- **Accessible** (data must be retrievable in order to be used and in order to assess it’s quality)
- **Timely** (recorded and available as soon after the event as possible)
- **Valid** (within an agreed format which conforms to recognised national standards)
- **Defined** (understood by all staff who need to know and reflected in procedural documents)
- ** Appropriately sought** (in terms of being collected or checked only once during an episode)
- ** Appropriately recorded** (in both paper and electronic records)

2.3.2 Staff should check with service users that the information held by the Trust is kept up to date by asking service users attending appointments to validate the information held.

2.3.3 Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/Personnel department. The Trust needs to ensure that cases are closed, when appropriate.

The GDPR (Articles 12,15,16,17,18,19,20,21,22,35) provide the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.
2.3.4 Some of these rights have to be determined by the courts and some are assessed on a case by case basis, but generally the Trust supports all of these principles.

2.3.5 Individuals whose information is held within the Trust have rights of access to it; regardless of the media the information may be held / retained.

Individuals also have a right to complain if they believe that the Trust is not complying with the requirements of the Data Protection legislation. *There are some exceptions to this, in the area of Mental Health.*

2.3.6 The Trust must ensure an up to date procedure is in place to deal with requests for access to information.

2.3.7 The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased service user’s records.

2.3.8 Individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress.

2.3.9 The Trust will ensure the complaints procedures are reviewed to take account of complaints which may be received because of a breach or suspected breach of the GDPR or DPA 2018.

2.4 The GDPR (Article 33, 34, 58, 83) requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used.

2.4.1 The Trust IM&T has a legal obligation to maintain confidentiality standards for all person identifiable information. This includes the disposal of non-clinical waste.

2.4.2 The Trust must ensure all electronic systems are maintained in line with the ISO/IEC 27000 series relating to Information Security Management.

2.5 The GDPR (Articles 45, 46, 49, 83, 84) imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

2.5.1 There is a statutory requirement for the Trust to notify the Information Commissioner, as part of the notification process, of any transfer of personal data to none EEA countries.
2.5.2 If you need to send person identifiable information to countries outside of the EEA you must discuss this with the Data Protection Officer, prior to any transfer taking place, as the levels of protection for the information may not be as comprehensive as those in the UK.

2.5.3 System Managers are required to check with software suppliers to ensure they conduct any development and bug fixes etc. within the UK or EEA. Where it is determined that any such development or support takes place in a country outside the EEA the Trust Data Protection Officer must be advised immediately. (See Appendix B)

2.5.4 It is advisable to check relevant, up to date information on this topic at, the Information Commissioners web site (www.ico.gov.uk) as part of risk assessment.

3.0 EXEMPTIONS

3.1 Article 23 enables Member States to introduce derogations to the GDPR in certain situations.

Member States can introduce exemptions from the GDPR’s transparency obligations and individual rights, but only where the restriction respects the essence of the individual's fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

- national security;
- defence;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences;
- other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
- the protection of judicial independence and proceedings;
- breaches of ethics in regulated professions;
- monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
- the protection of the individual, or the rights and freedoms of others; or
- the enforcement of civil law matters.

There are specific reasons why access to personal data may be denied including:
- Where the data released may cause serious harm to the physical or mental condition of the patient, or any other person.
- Where access would disclose information relating to or provided by a third party (where consent has not been received by the third party to release their data). NB this does not include information recorded by the Trust employees as part of their normal duties.
- Where it is assessed that a patient, under the age of 16, cannot understand the implications of accessing their records.

(Note: refer to Access to Records Procedure (CPG9d))
4.0 RETENTION OF INFORMATION

4.1 The Trust will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will either be archived or destroyed. This will be done in accordance with the reasonable retention periods detailed in the Trust’s Storage, Retention and Destruction of Records Procedural Guidelines (CPG9), which is compliant with the Department of Health Records Management NHS Code of Practice Part II, second edition 2009, and the Codes of Practice for the Management of Records Section 46 of the Freedom of Information Act 2000.

5.0 REPORTING BREACHES

5.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Any potential or actual breaches must be reported to the line manager immediately.

5.2 The Information Governance Team should be notified and a DATIX incident report completed. The Information Governance Team will be able to give advice on how to rectify / reduce the impact of the breach.

In the event of the loss of Trust equipment, IT need to be informed as soon as possible.

(Note: refer to Information Security Incident Reporting Procedure (CPG50d)

6.0 TRAINING AND SUPPORT

6.1 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 Website.
- Training via the Trusts’ e-learning programme (OLM)
- 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 (HR21).
7.0 MONITORING AND REVIEW

7.1 This procedural guideline will be reviewed in line with its associated policy document and/or whenever changes in legislation, guidance from Department of Health, the NHS Executive or the Information Commissioner’s Office require.

7.2 The Executive Medical Director is responsible as the Caldicott Guardian in association with the SIRO for the implementation of these procedural guidelines and its associated policy document.

END
CONFIDENTIALITY PROCEDURE

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER:</th>
<th>CPG59b</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>5</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td>Made compliant with GDPR</td>
</tr>
<tr>
<td>AUTHOR:</td>
<td></td>
</tr>
<tr>
<td>CONSULTATION GROUPS:</td>
<td>IGSSC</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>MAY 2018</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td>March 2018; August 18</td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>N/A</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>October 2019</td>
</tr>
<tr>
<td>APPROVAL BY IGSSC COMMITTEE:</td>
<td>July 2018</td>
</tr>
<tr>
<td>COPYRIGHT</td>
<td>© Essex Partnership University NHS Foundation Trust 2017. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner</td>
</tr>
</tbody>
</table>

POLICY SUMMARY

The purpose of this Procedure is to ensure that staff understand their responsibilities regarding the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 ("DPA"), thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the "Trust").

The Trust monitors the implementation of and compliance with this policy 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.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is Chief Finance Officer
1.0 INTRODUCTION
2.0 CONFIDENTIALITY GUIDANCE SECTION
3.0 CALDICOTT PRINCIPLES
4.0 THIRD PARTY REQUESTS FOR CONFIDENTIAL INFORMATION
5.0 REPORTING BREACHES OF CONFIDENTIALITY
6.0 TRAINING AND SUPPORT
7.0 MONITORING AND REVIEW
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY PROCEDURE

Assurance Statement
The purpose of this Procedure is to ensure that all staff understand their responsibilities regarding confidentiality of data, thereby ensuring that lawful and correct processing of personal information is a key part of building and maintaining trust and confidence in Essex Partnership University NHS Foundation Trust (the “Trust”).

1.0 INTRODUCTION

1.1 All legislation relevant to an individual’s right to confidentiality and the ways in which that can be achieved and maintained are paramount to the Trust. This relates to roles that are reliant upon computer systems such as: service user administration, payment, purchasing, invoicing and treatment planning. Legislation also regulates the use of manual records relating to service users, staff and others whose information may be held within the Trust.

1.2 Patients expect that information about them will be treated as confidential and are given that assurance in the Patient Charter (1997), ‘everyone working for the NHS is under a legal duty to keep your records confidential.’ Patients who feel that confidence has been breached may issue a complaint under the NHS complaints procedure or they could take legal action.

2.0 CONFIDENTIALITY GUIDANCE SECTION

2.1 Access to Confidential Information

2.1.1 It is the Trust’s responsibility to protect the rights of patients, staff and individuals, who expect confidentiality of personal information held and processed by the Trust.

2.1.2 The Trust expects that all employees ensure that all confidential information attained in the course of their work is treated in strict confidence, and is in addition to responsibilities associated with individual professional codes of practice.

2.1.3 It will be the individual responsibility of all service managers to keep all confidential information safe and secure and identify measures within their own area of responsibility, which limit access to information to authorised personnel only.

2.1.4 All information obtained by Trust employees in the course of their work may only be disclosed to third parties with the express consent of the individual and as authorised by the Trust, or where required by order of a court or where
it can be justified in the wider public interest under the General Data Protection Regulation.

2.1.5 Any decision to disclose confidential information about a patient’s treatment or care should always, in the first instance, be brought to the attention of the patient’s Responsible Medical Officer. It will be their responsibility to assess whether disclosure of information is in the interests of the patient and liaison with the person in charge, decide whether the patient is able to give informed consent. Any decision relating to the disclosure of personal data about a patient to a third party, whether that disclosure is verbal or written, should be recorded in the patient’s health records.

2.1.6 If any doubt exists concerning the nature of information being classified as confidential, Trust employees are advised to treat the information as confidential and seek clarification from their service manager or the Trust’s Data Protection Officer, before disclosing information.

2.1.7 Any disclosure of confidential information, not in accordance with the terms of these guidelines or its associated policy, will be viewed as a serious breach of discipline and will be dealt with under the Trust’s disciplinary rules and procedures.

2.2 Requests for Confidential Information

2.2.1 All requests for confidential information concerning a patient, staff or other individual, including requests from third parties, must be passed to the appropriate service manager, who will be responsible dealing with the matter, adhering to the guidelines set out within this policy. Further clarification and advice may be sought from the Trust’s Information Governance Team or Data Protection Officer.

3.0 CALDICOTT PRINCIPLES

3.1 The Caldicott Principles were developed in 1997 following a review of how patient information was handled across the NHS. The Review Panel was chaired by Dame Fiona Caldicott and it set out six Principles that organisations should follow to ensure that information that can identify a patient is protected and only used when it is appropriate to do so. Since then, when deciding whether they needed to use information that would identify an individual, an organisation should use the Principles as a test. The Principles were extended to adult social care records in 2000.
The Caldicott Principles (revised 2013) are:

**Principle 1 - Justify the purpose(s) for using confidential information**

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2 - Don't use personal confidential data unless it is absolutely necessary**

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3 - Use the minimum necessary personal confidential data**

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4 - Access to personal confidential data should be on a strict need-to-know basis**

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities**

Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6 - Comply with the law**

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality (added in 2013)**

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
4.0 THIRD PARTY REQUESTS FOR CONFIDENTIAL INFORMATION

4.1 In cases where requests for confidential information about a patient are made from a third party, the patient will be informed unless it can be demonstrated by the patient’s Responsible Medical Officer and / or the Trust’s nominated representatives that it is not in the interests of the patient to do so.

4.2 It will be the normal practice of designated Trust employees to record requests for confidential information from third parties and this should be recorded in the patient’s health records along with the actions taken as a result of the request.

5.0 REPORTING BREACHES OF CONFIDENTIALITY

5.1 Any potential or actual breaches of confidentiality must be reported to the line manager immediately.

5.2 The Information Governance Team should be notified and a DATIX incident report completed. The Information Governance Team will be able to give advice on how to rectify / reduce the impact of the breach.

(Note: refer to Information Security Incident Reporting Procedure (CPG50d)

6.0 TRAINING AND SUPPORT

6.1 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 Trust Today, Viewpoint and others
- On-Line training via the NHS Digital website.
- Training via the Trust’s e-learning programme (OLM)
- 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 (HR21).

7.0 MONITORING AND REVIEW

7.1 This procedural guideline will be reviewed in line with its associated policy document and / or whenever changes in legislation, guidance from Department of Health, the NHS Executive or the Information Commissioner’s Office require.
7.2 The Chief Finance Officer is responsible (as the Trust SIRO) with the Caldicott Guardian for the implementation of these procedural guidelines and its associated policy document.

END
CONFIDENTIALITY AUDIT PROCEDURE

PROCEDURE REFERENCE NUMBER: CPG59c
VERSION NUMBER: 3
KEY CHANGES FROM PREVIOUS VERSION: GDPR updates
AUTHOR: Information Governance Manager
CONSULTATION GROUPS: Information Governance Steering Committee; C Aldicott Network; Clinical / Operational Leads
IMPLEMENTATION DATE: April 2017
AMENDMENT DATE(S): October 2017
LAST REVIEW DATE: August 2018
NEXT REVIEW DATE: March 2021
APPROVAL BY IGSSC: September 2018
RATIFICATION BY QUALITY COMMITTEE: TBC
COPYRIGHT: © Essex Partnership University NHS Foundation Trust 2018. All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

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

The Trust monitors the implementation of and compliance with this policy in the following ways:
Auditing and Datix reporting to monitor the compliance with confidentiality across the Trust.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

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

1.0 INTRODUCTION
2.0 SCOPE
3.0 RESPONSIBILITIES
4.0 MONITORING ACCESS TO CONFIDENTIAL INFORMATION
5.0 MONITORING & REVIEW
6.0 REFERENCE TO OTHER DOCUMENTATION
CONFIDENTIALITY AUDIT PROCEDURE

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

Please read in conjunction with the Data Protection Act 2018 and Confidentiality Policy and associated procedures.

1.0 INTRODUCTION

1.1 Advances in electronic management of health and employment records / information within the NHS has resulted in the requirement to monitor access to such confidential systems and therefore the information governance agenda requires that all organisations that handle person identifiable information have arrangements in place to manage and safeguard confidentiality.

1.2 As large numbers of staff use these systems it is imperative that access is monitored and controlled and the Trust should, therefore, as best practice, have processes to highlight actual or potential confidentiality breaches in their systems, particularly where person identifiable information is held.

2.0 SCOPE

2.1 These procedures must be adhered to by all staff (including permanent/contract/agency/locum/trainees etc.) using Trust information systems / processes where person identifiable information / data is held.

2.2 This procedure covers all forms of information / data, including paper, electronic, digital, etc.

3.0 RESPONSIBILITIES

3.1 Caldicott Guardian / Deputy Caldicott Guardian

3.1.1 The Caldicott Guardian will be informed of any serious breaches of confidentiality in regard of patient identifiable information and act accordingly.
3.2 **Senior Information Risk Officer / Deputy Senior Information Risk Officer**

3.2.1 The Senior Information Risk Officer will be informed of any breaches of confidentiality in regard of person identifiable information and act accordingly.

3.3 **Information Governance Manager**

3.3.1 The Information Governance Manager will, in conjunction with the appropriate managers / leads for the individual systems set up processes for undertaking the monitoring audits on a regular basis (i.e. annually/bi-annually/quarterly/bi-monthly/monthly).

3.3.2 The key leads will provide reports to the Information Governance Manager on the outcomes of these audits and advise of any anomalies which may be considered breaches for investigation, and where processes may need to be changed or improved.

3.3.3 The Information Governance Manager will ensure that the Caldicott Guardian and / or Senior Information Risk Officer are apprised on breaches, investigations and outcomes, as appropriate, providing advice and guidance where necessary.

3.3.4 The Information Governance Team is responsible for the definition, implementation and monitoring of the Information Asset Register (IAR).

3.4 **Privacy Officer**

3.4.1 The Information Governance Manager is the designated Privacy Officer for the Trust.

3.4.2 The Privacy Officer will receive automatic alerts concerning access to the systems / processes where a legitimate relationship does not exist.

3.5 **Data Protection Officer**

3.5.1 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 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.
3.6 Information Security Officers

3.6.1 The Associate Director of IT Strategy & Technical Projects is the Trust’s designated Information Security Manager. They will work closely to ensure the implementation of information governance / security practices across the organisation. Attending the Information security Forum on a regular basis and through the Forum maintaining the Trust’s Security risk register.

4.0 MONITORING ACCESS TO CONFIDENTIAL INFORMATION

4.1 In order to provide assurance that access to person identifiable information is gained only by those individuals that have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

4.2 The Information Governance Team and the Caldicott Guardian / Senior Information Risk Officer will decide on any actions to be taken to address anomalies identified, through the implementation of, for example:

- Additional controls
- Restriction of access
- Investigation
- Presentation of investigation outcomes with recommendations for further action such team working processes, recommended disciplinary action, additional training needs etc.

Outcomes of these discussions and actions to be taken will be fed back to the key leads by the Information Governance Team.

4.3 Any anomalies (evidence of improper use of systems / libraries; change of role requiring adjustment to access, etc.) – will be reported via Datix and investigation through the normal channels of information incidents investigation (see also Reporting Information Incidents procedure).

4.4 Monitoring will include, but not be limited to, review / audit of:

- Failed attempts to access person identifiable information by an unauthorised person/s
- Repeated attempts to access person identifiable information by an unauthorised person/s
- Successful access of person identifiable information by unauthorised person/s
- Evidence of shared login sessions / passwords
- Access to potential family and friends / neighbours and colleagues information
- Creating / deleting / altering records for the purposes of inappropriate use and without approval
- Overriding consent

4.5 Monitoring will take place across a range of systems / access routes to person identifiable information, for example:

- PARIS
- Intranet Client Information
- Smart Card access
- ESR (Electronic Staff Records)
- Paper Records (from records tracer)
- SystmOne
- Mobius
- Networks
- Closed account emails / open account (leavers)

*This list is not-exhaustive.*

4.6 Monitoring will consist of random checks within the systems (as above 4.6).

4.7 Breaches of confidentiality, reported via Datix, will be investigated and the Trust systems may be interrogated as part of that investigation to identify whether unauthorised access has occurred.

4.8 In addition the Information Governance Team will regularly carry out spot-check audits of services, teams to review compliance to Trust policy, local and national guidance around the protection of information / data / systems.

4.9 Results of all audits are fed back to the team managers, where anomalies, breach of confidentiality or non-adherence to policy is identified for further action and investigation. The outcome of the investigations will be reported back to the Information Governance Team.

4.10 All suspected breaches / unauthorised access to confidential information systems will be investigated. This may result in further investigation under the Trust’s disciplinary or conduct & capability procedures.

5.0 MONITORING AND REVIEW

5.1 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.
5.2 Compliance to this procedure will be undertaken in line with Trust policy and timetables for compliance audits.

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

6.0 REFERENCE OTHER DOCUMENTATION

- Trust Information Governance & Security Policy and associated procedures
- Trust Records Management Policy and associated procedures
- NHS Information Governance Toolkit
- NHS Confidentiality Code of Conduct
- Registration Authority Governance Arrangements for NHS Organisations
- Caldicott Principles
- Data Protection Directive
- Data Protection Act 2018
- Computer Misuse Act 1990
- Health & Social Care Act 2012
- Human Rights Act 1998
- NHS Constitution
- General Data Protection Regulation

This list is not exhaustive.

END
<table>
<thead>
<tr>
<th>Hospital No:</th>
<th>No of Pages</th>
<th>OK or not</th>
<th>Error Code</th>
<th>Action Required:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Any document changes must be done in both Legal and Legal repository:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code:</th>
<th>Count:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Date Error</td>
</tr>
<tr>
<td>B</td>
<td>Case Sender / Case Recipient error</td>
</tr>
<tr>
<td>C</td>
<td>Wrong document Type</td>
</tr>
<tr>
<td>D</td>
<td>Test or barcode covered (lost, torn, misplaced)</td>
</tr>
<tr>
<td>E</td>
<td>Bar Code being scanned (outside frame, Failed)</td>
</tr>
<tr>
<td>F</td>
<td>2-3-4 sheets scanned together:</td>
</tr>
<tr>
<td>G</td>
<td>All scanner failure (missing &amp; recycled paper used)</td>
</tr>
<tr>
<td>H</td>
<td>Other:</td>
</tr>
<tr>
<td>I</td>
<td>Printing issues (Low ink, Leaking ink, Bar Code Failed)</td>
</tr>
<tr>
<td>J</td>
<td>Other printing issues</td>
</tr>
<tr>
<td>K</td>
<td>Document partly scanned:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code:</th>
<th>Count:</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>Document Not found, Re-Scanned</td>
</tr>
<tr>
<td>M</td>
<td>2 or more patients scanned in the same Doc.</td>
</tr>
<tr>
<td>N</td>
<td>Document Not Scanned to Scanning Folder</td>
</tr>
<tr>
<td>O</td>
<td>2 or more different documents for the same patient scanned together:</td>
</tr>
<tr>
<td>P</td>
<td>Wrong Bar coded Coversheet printed and scanned for the wrong Patient:</td>
</tr>
<tr>
<td>Q</td>
<td>Scannable failures (Barcodes damaged, torn, double image, punched, angled, glass dirty)</td>
</tr>
<tr>
<td>R</td>
<td>Scanned Single Sided, Re-Scanned</td>
</tr>
<tr>
<td>S</td>
<td>Documents In Failed Folder:</td>
</tr>
</tbody>
</table>
NOTICE

THE FOLLOWING PAGE(S) ARE TORN OR DAMAGED
THEY HAVE BEEN SCANNED AS PER THE ORIGINAL(S)
<table>
<thead>
<tr>
<th>PLEASE DO:</th>
<th>PLEASE DO NOT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Keep records in an organised filing system, with individual files recorded in a log or register; ideally each Department should have a central shared filing system in place for its paper records</td>
<td>✗ Keep records in desk drawers or stack them on the floor</td>
</tr>
<tr>
<td>✓ Within the Register, a Disposal Review date should be calculated Based on the rules within the retention schedules contained in the Records Management: NHS Code of Practice (this date should also be added to the file cover sheet)</td>
<td>✗ Guess at retention periods</td>
</tr>
<tr>
<td>✓ Keep person-identifiable and commercially sensitive confidential records in a locked cabinet</td>
<td>✗ Keep confidential records in open cupboards</td>
</tr>
<tr>
<td>✓ Confidential records must be marked on the file cover sheet in the Protective Marking field – identify as ‘extremely sensitive’, ‘sensitive’ or ‘ordinary’¹</td>
<td>✗ Store records on window sills</td>
</tr>
<tr>
<td>✓ Scan all important paper records, saving them to the Laserfiche EDRM system (or a network drive if you do not yet make use of Laserfiche)</td>
<td></td>
</tr>
<tr>
<td>✓ Use a space-efficient filing system - lateral shelf filing, using landscape box or hanging files to increase the number of shelves in the height available</td>
<td>✗ Use lever arch files wherever possible as these are inefficient to store and costly to buy</td>
</tr>
<tr>
<td>✓ Where you have a large number of files, consider colour-coded labels to visually assist file location and retrieval</td>
<td></td>
</tr>
<tr>
<td>✓ Consider the physical and environmental protection of records (in addition to security controls)</td>
<td>✗ File records where there is any risk of fire, flood, damp, humidity, pest attack and general damage</td>
</tr>
<tr>
<td>✓ Consider Health &amp; Safety when managing files, including the height of shelving and weight of files / boxes</td>
<td>✗ Use the same file when it is too bulky (over 4 cm thick) - open a new file/volume, and refer to the older file on the cover</td>
</tr>
<tr>
<td>✓ Keep frequently accessed, large or heavy files below knee or above shoulder height</td>
<td></td>
</tr>
</tbody>
</table>

¹ Class 1 – extremely sensitive: where information held is of a highly sensitive nature and where security is at the highest level (e.g. internal security documentation)

Class 2 – sensitive: Where information is not of the most sensitive nature but still requires strict security (e.g. trade secrets, foreign affairs)

Class 3 – ordinary/confidential: where information is not patient based but security measures are required (e.g. Human Resource information)
<table>
<thead>
<tr>
<th>PLEASE DO:</th>
<th>PLEASE DO NOT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Where structured paper files are still maintained, as well as paper</td>
<td>❌ Overfill archive boxes; keep to a 12kg limit for health and safety reasons</td>
</tr>
<tr>
<td>originals, please print and add to the file all e-mails and network</td>
<td></td>
</tr>
<tr>
<td>drive documents relevant to the ongoing story</td>
<td></td>
</tr>
<tr>
<td>✓ Retain records in a chronological order, with the earliest paper at</td>
<td>❌ Destroy the electronic originals: this is particularly important for email</td>
</tr>
<tr>
<td>the back of the file, working to the most recent paper at the front.</td>
<td>as a paper copy of an email may not be valid in law because a lawyer</td>
</tr>
<tr>
<td></td>
<td>can suggest that it was altered prior to printing.</td>
</tr>
<tr>
<td>✓ File covers should be sturdy, secure and convenient to handle</td>
<td>✓ Use rubber bands or sellotape to hold files together, plastic A4 wallets</td>
</tr>
<tr>
<td></td>
<td>and covers, metal fastenings (except for brass paperclips), which can all</td>
</tr>
<tr>
<td></td>
<td>degrade files/papers</td>
</tr>
<tr>
<td>✓ Ensure the file cover sheet is completed and attached</td>
<td>✓ Use post-it notes to record information in a file – they are easily removed</td>
</tr>
<tr>
<td></td>
<td>and lost</td>
</tr>
<tr>
<td>✓ Arrange and sequence files via a logical referencing system to meet</td>
<td>❌ Maintain files containing records of differing retention periods wherever</td>
</tr>
<tr>
<td>business and retrieval needs, which will be easily understood by</td>
<td>possible or practical</td>
</tr>
<tr>
<td>staff members; this could be a simple alphabetical system, or a more</td>
<td></td>
</tr>
<tr>
<td>complex alphanumeric referenced system</td>
<td></td>
</tr>
<tr>
<td>✓ Please arrange files with retention schedules in mind (this will make</td>
<td>❌ Begin a new file with a paper referring to another paper that is not on</td>
</tr>
<tr>
<td>review for disposal much easier) - you should separate closed files</td>
<td>that file.</td>
</tr>
<tr>
<td>and arrange these in date order</td>
<td></td>
</tr>
<tr>
<td>✓ 'Vital' records (which are essential to the legal and fiscal running</td>
<td>❌ Throw weeded file contents in ordinary rubbish bins</td>
</tr>
<tr>
<td>of the Trust) must be scanned and stored in a fire rated room/cabinet</td>
<td></td>
</tr>
<tr>
<td>✓ When a file is closed, this should be clearly marked on the file cover,</td>
<td></td>
</tr>
<tr>
<td>a reference to the new file marked on the closed file, and a reference</td>
<td></td>
</tr>
<tr>
<td>to the closed file marked on the new file.</td>
<td></td>
</tr>
<tr>
<td>✓ Weed (or cleanse) files before closure: as much as 40% of the material</td>
<td></td>
</tr>
<tr>
<td>in an average file will often be unnecessary to retain in the longer</td>
<td></td>
</tr>
<tr>
<td>term, especially duplicate copies - weeded documents must be securely</td>
<td></td>
</tr>
<tr>
<td>disposed of</td>
<td></td>
</tr>
<tr>
<td>✓ Consider archiving files away from premium office space once closed</td>
<td>❌ Use of non-specific or generic terms, such as “general correspondence” or</td>
</tr>
<tr>
<td></td>
<td>“miscellaneous”</td>
</tr>
<tr>
<td></td>
<td>❌ Use acronyms and abbreviations that are not in common use within the Trust</td>
</tr>
<tr>
<td></td>
<td>❌ Use file titles worded so that personal / confidential information (address or telephone number, phrases such as “vexatious litigant” etc.) is included in the title</td>
</tr>
<tr>
<td>PLEASE DO:</td>
<td>PLEASE DO NOT:</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>currently have use of the file</td>
<td>x Records should never be left in ordinary rubbish bins, open skips or where it might be vulnerable to casual retrieval</td>
</tr>
<tr>
<td>✓ When returning a file, update the register and remove the tracer card</td>
<td></td>
</tr>
<tr>
<td>✓ If records become eligible for disposal retention schedules contained in the <em>Records Management: NHS Code of Practice</em>, they should be shredded and disposed of as confidential waste</td>
<td></td>
</tr>
<tr>
<td>✓ No records should be destroyed without managerial approval and consultation with the Trust Records Group</td>
<td></td>
</tr>
<tr>
<td>✓ All disposal actions should be recorded in the File Register</td>
<td></td>
</tr>
</tbody>
</table>
# Do’s and Don’ts for Electronic Filing Practices

<table>
<thead>
<tr>
<th>PLEASE DO:</th>
<th>PLEASE DO NOT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Prior to being finalised records stored in Laserfiche, please file electronic documents using your network user account, within a shared drive (e.g. H:, S:, T:)</td>
<td>❌ Use the C:\ drive; My Documents / Pictures / Desktop, data sticks or CD’s as these are not secure and could compromise patient, staff or Trust sensitive information</td>
</tr>
<tr>
<td>✓ However, you may wish to make use of Laserfiche’s use of the system’s imaging, search, workflow and version control capabilities and thus file documents in the system when created</td>
<td></td>
</tr>
<tr>
<td>✓ Where an electronic file is maintained, please file together both electronic documents (in their original format) and scanned images of paper originals to form the complete narrative</td>
<td></td>
</tr>
<tr>
<td>✓ It is important to save electronic copies of emails (in .msg format) that document business decisions, activities and transactions in a folder together with the other records which form part of the same narrative and can also be subject to the same retention and disposal rules and processes</td>
<td>❌ Use the email system as a permanent record store for significant documents and information</td>
</tr>
<tr>
<td>✓ If attachments are important they should be saved separately (as well) so that they can be readily located - indeed it will not always be necessary to save the actual message if the content is not significant, although in many cases the email message will provide the context within which the attachment was used</td>
<td>❌ File non-important emails of a routine/transitory nature - you should not keep (or forward) junk or chain mail</td>
</tr>
<tr>
<td>✓ Arrange and name folders based on a hierarchy (please see illustrated example above) from the general to the specific, representing the Trust’s business functions and activities - potentially use the higher level folders as descriptive categories, filing records in the lower level folders representing specific tasks</td>
<td></td>
</tr>
<tr>
<td>✓ The folder title must readily identify the single task or topic for the records it will contain</td>
<td>❌ Use folder names such as ‘general’, ‘miscellaneous’, ‘John’s file’, ‘Jane’s work’, which are unhelpful and must be avoided</td>
</tr>
<tr>
<td>✓ As a general tip, alphabetic folder names are generally more usable; 16-20 characters should be adequate for a folder name</td>
<td></td>
</tr>
<tr>
<td>✓ Please note that all records should be saved in native formats (Word, Excel, Outlook .msg etc.)</td>
<td></td>
</tr>
<tr>
<td>✓ FINAL versions of published documents could also be saved in non-editable pdf formats to ensure long term integrity / accuracy and prevent accidental corruption</td>
<td></td>
</tr>
<tr>
<td>✓ Based on the file naming convention above, working drafts should be given a minor version number (e.g. v0.1, v0.2 etc.) and, when finalised, the working drafts deleted (unless there is a</td>
<td>❌ Use the Microsoft Word versioning tool, as this function substantially increases the size of your document which in turn wastes valuable server space</td>
</tr>
<tr>
<td>PLEASE DO:</td>
<td>PLEASE DO NOT:</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>need for proof of process)</td>
<td></td>
</tr>
<tr>
<td>✓ The finalised version would be titled Version 1.0. If version 1.0 is</td>
<td>✗ Use words such as 'the', 'a', 'and', 'if', 'but', 'so', 'for', 'general'</td>
</tr>
<tr>
<td>to be revised, drafts would be numbered as 1.1, 1.2... until Version 2.0</td>
<td>✗ Use non alphanumeric characters such as * : \ / &lt;&gt; &quot; [ ] ; = + £ $ .</td>
</tr>
<tr>
<td>is complete - use the 'save as' function to create new versions</td>
<td>✗ Use of initials, acronyms, abbreviations and codes that are not commonly</td>
</tr>
<tr>
<td>✓ All final versions of documents should be saved in Laserfiche</td>
<td>understood or part of a controlled vocabulary</td>
</tr>
<tr>
<td>✓ Where available, templates should be used for creating new documents</td>
<td>✗ Re-use the names of the folder structure in which the record resides</td>
</tr>
<tr>
<td>✓ If the document is of a restricted class¹, add 'Confidential and</td>
<td>✗ Put file format types, e.g. Presentation or Document, in the name</td>
</tr>
<tr>
<td>Commercially Sensitive' to the document header</td>
<td>✗ Use punctuation (use a hyphen if required to give meaning / separate</td>
</tr>
<tr>
<td>✓ Use the file naming convention shown in section 7 above, selecting</td>
<td>concepts)</td>
</tr>
<tr>
<td>those elements which are applicable - Keep file names short, but</td>
<td></td>
</tr>
<tr>
<td>meaningful, using keywords relating to the subject</td>
<td></td>
</tr>
<tr>
<td>✓ Use capital letters to delimit words</td>
<td></td>
</tr>
<tr>
<td>✓ Avoid unnecessary repetition and redundancy in file names and file</td>
<td></td>
</tr>
<tr>
<td>paths - ideally this means you should not have to re-use the names of</td>
<td></td>
</tr>
<tr>
<td>the folder structure in which the record resides</td>
<td></td>
</tr>
<tr>
<td>✓ When including a personal name in a file name give the family name</td>
<td></td>
</tr>
<tr>
<td>first followed by the initials / forename</td>
<td></td>
</tr>
<tr>
<td>✓ Add/update the file name and number of pages into the document footer</td>
<td></td>
</tr>
<tr>
<td>✓ Use the document Properties to describe the context of the document</td>
<td></td>
</tr>
<tr>
<td>version.</td>
<td></td>
</tr>
<tr>
<td>✓ Check the Author's name and Company reference in the document</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td></td>
</tr>
<tr>
<td>✓ Check any document control information and update the table of</td>
<td></td>
</tr>
<tr>
<td>contents</td>
<td></td>
</tr>
<tr>
<td>✓ If records become eligible for disposal</td>
<td></td>
</tr>
<tr>
<td>retention schedules contained in the Records Management: NHS Code of</td>
<td></td>
</tr>
<tr>
<td>Practice, they should be destroyed by IT</td>
<td></td>
</tr>
<tr>
<td>✓ All disposal actions for documents filed on the network should be</td>
<td></td>
</tr>
<tr>
<td>recorded (This will happen automatically within the Laserfiche audit</td>
<td></td>
</tr>
<tr>
<td>trail)</td>
<td></td>
</tr>
</tbody>
</table>

¹ Class 1 – extremely sensitive: where information held is of a highly    |
| sensitive nature and where security is at the highest level (e.g. internal |
| security documentation)                                                    |

Class 2 – sensitive: Where information is not of the most sensitive nature |
| but still requires strict security (e.g. trade secrets, foreign affairs)   |

Class 3 – ordinary/confidential: where information is not patient based but 
| security measures are required (e.g. Human Resource information)            |
PAPER AND ELECTRONIC CORPORATE RECORDS PROCEDURE

POLICY REFERENCE NUMBER: CPG61

VERSION NUMBER: 5

KEY CHANGES FROM PREVIOUS VERSION: Incorporated new General Data Protection Regulations. Included the definition of a missing record.

AUTHOR: Records Manager

CONSULTATION: Information Governance Steering Committee, Quality Committee, Paris Project Board, Mobius Project Board

IMPLEMENTATION DATE: April 2017

AMENDMENT DATE(S): August 2018; March 19

LAST REVIEW DATE: June 19

NEXT REVIEW DATE: August 2022

APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE: March 2019

RATIFIED BY QUALITY COMMITTEE: June 2019

COPYRIGHT: © EPUT 2018 All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

OPERATIONAL POLICY SUMMARY

The purpose of this Procedural Guideline document is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of electronic and paper corporate records.

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

This process is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee.

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer.
<table>
<thead>
<tr>
<th>CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 INTRODUCTION</td>
</tr>
<tr>
<td>2.0 PURPOSE</td>
</tr>
<tr>
<td>3.0 RESPONSIBILITY</td>
</tr>
<tr>
<td>4.0 DOCUMENTS AND RECORDS</td>
</tr>
<tr>
<td>5.0 FILING PAPER RECORDS</td>
</tr>
<tr>
<td>6.0 ACCESS CONTROL TO THE LASERFICHE SYSTEM</td>
</tr>
<tr>
<td>7.0 FILING ELECTRONIC RECORDS</td>
</tr>
<tr>
<td>8.0 PRESERVATION OF RECORDS</td>
</tr>
<tr>
<td>9.0 DOCUMENT SCANNING</td>
</tr>
<tr>
<td>10.0 ELECTRONIC RECORD RETRIEVAL</td>
</tr>
<tr>
<td>11.0 ELECTRONIC RECORD DISPOSAL</td>
</tr>
<tr>
<td>12.0 REFERENCE TO OTHER POLICIES AND PROCEDURES</td>
</tr>
</tbody>
</table>

**APPENDICES**

APPENDIX A - QUALITY ASSURANCE FORMS

APPENDIX B - NOTICES (PHOTOCOPIES/TEAR/DAMAGED DOCUMENTS)

APPENDIX C - DO’S AND DON’TS FOR PAPER FILING PRACTICES

APPENDIX D - DO’S AND DON’TS FOR ELECTRONIC FILING PRACTICES
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PAPER AND ELECTRONIC CORPORATE RECORDS
(LASERFICHE) PROCEDURE

Assurance Statement

The purpose of these procedure guidelines is to ensure that the Trust efficiently and effectively manages the creation, filing, retrieval, appraisal, archive and destruction of electronic and paper corporate records. These guidelines are implemented in adherence to the NHS Connecting for Health Information Governance Toolkit Requirement 601 “Documented and implemented procedures are in place for the effective management of corporate records”, as well as in accordance with the Records Management: NHS Code of Practice, and other relevant guidance and legislation and general good practice in records management.

1.0 INTRODUCTION

1.1 Rising costs of archive storage means The Trust has needed to look at alternatives for timely and accurate access to records.

1.2 The Trust has therefore introduced an electronic storage and retrieval system which will underpin its corporate record management strategy for the future.

1.3 There are a number of benefits to be gained from the gradual movement of paper records to electronic records:

- Reduces filing / storage space by the removal of existing filing racks and cabinets freeing up space for other purposes
- Central record of relevant files
- Meets the health and safety and legislative and other storage criteria set for NHS organisations
- Improves Trust wide access to files and documents
- Reduces the incidences of lost / missing files and provides concrete disaster contingency
- Moves the Trust in the direction of full electronic corporate records

2.0 PURPOSE

2.1 The purpose of this procedure is to enable all staff to understand:

- The difference between a document and a record
- Where and how a record should be filed
- The referencing to be applied to new records
- The naming conventions in use in the Trust
- Version control standards
- If appropriate, how to apply a protective mark
3.0 RESPONSIBILITY

3.1 The Director of ITT is responsible for Trust wide and strategic management of records. In addition the Trust has nominated officers (Head of Electronic Systems & Records / Records Manager) responsible for ensuring compliance with Trust policy and for ensuring records are stored and destroyed in line with Trust policy.

3.2 All staff are responsible for the management of records within their area of activity irrespective of media.

4.0 DOCUMENTS AND RECORDS

Definition of a Record:-

4.1 Records are defined as ‘recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity’.

4.2 These can be primary, management or support activities. They are kept as audit trail evidence of and information about the Trust’s functions, decisions, processes, procedures, operations, proper conduct, rights and obligations, transactions or other activities of the organisation.

4.3 Records can exist in any medium and format, both electronic and hard copy, including but not restricted to e-mail messages, word processing and spreadsheet documents, presentations, PDFs, desktop publishing, scanned images, instant messages, audio, video, databases, electronic forms, computer reports, photographs, CAD and maps.

When does a Document become a Record?

4.4 Not all documents and information are designated as records which must be managed according to Trust policy and procedure. A document becomes a record when:
- It represents evidence of an activity as described above; and
- It is finalised and becomes part of the Trust’s corporate information

4.5 The following documents will almost certainly become records:
- Action Plans
- Building/structural work, property maintenance/repairs, engineers inspection reports
- Business plans/business cases
- Commissioned Services
- Committees, Agendas, Minutes and Terms of Reference
- Communications/public relations communiqués
- Complaints papers and correspondence
- Contract and Tendering records
- COSHH and other Health & Safety records
- Financial records / papers
- Industrial Relations documents
- Information Governance Toolkit Evidence
• Internal/External Assurances records
• Major events/notable events (e.g. major incidents, including pandemics, or substantial changes in the provision of local healthcare)
• Major projects and plans (e.g. opening of new buildings; healthcare plans/strategies)
• Ministerial submissions and advice
• Minutes of significant meetings (i.e. where significant decisions are made)
• Papers relating to the preparation of legislation
• Performance monitoring
• Personnel records
• Policies and Strategies
• Policy development documents, reports and correspondence
• Procurement records (e.g. contracts)
• Project Initiation documents (e.g. strategy; requirements, PID, sign off, project review)
• Reports
• Research and development papers
• Superannuation records
• Training records

*This list is not exhaustive....*

4.6 It should be noted that drafts should also be treated as formal records when there is a need for proof of process and the capability to show how ideas developed over time and in response to specific events. Once a document becomes a record, it should not be amended and should only be held in the corporate Electronic Document Records Management System (EDRM) system (or a network drive if you do not yet make use of the corporate EDRM) if electronic, or within a managed filing system if paper. All records should also be retained in line with the retention schedules contained in the Information Governance Alliance Records Management Code of Practice 2015.

**When does a document become a record?**

A document becomes a true record when it is saved and could be via any of the following methods:

• when the document has finished being a draft version e.g. becomes version 1.0 as opposed to 0.1
• when the document has been approved as a true record, e.g. draft minutes are signed off
• When a person decides that a document has to be kept, e.g. as evidence
How should Non-Records be handled?

4.7 Not all information is an evidential record. Papers should not be filed if not worth filing and documents should not be kept ‘just in case’. Generally speaking, information that is duplicated, printed from electronic sources for facilitative reasons, out-of-date or superseded and kept for reference rather than evidence, can be discarded once business use has finished. Staff should ensure that these are recycled or if appropriate destroyed as confidential waste. Examples include:

- Junk mail
- Copies of master records
- Drafts printed for proof-reading
- Old forms
- Stationery
- ‘With compliments’ slips (unless used to convey information)
- Catalogues and trade journals
- Non-acceptance of invitations / invitations for events in the past
- Trivial electronic mail messages or notes that are not related to Trust business
- Requests for routine information
- Out-of-date distribution lists

This list is not exhaustive....

Definition of a missing record:

A ‘misplaced’ record is a record that either cannot be found or is unavailable within 5 working days following the first attempt to access that record when required for an out-patient appointment, admission, other patient contact, or for a serious incident.

A record is considered ‘missing’ (internally only) when the original file has not been located following all investigations, as detailed in these procedures.

A record is not considered as being ‘lost’ e.g. notifiable to the patient (if applicable) until a period of six months has elapsed from the time the record was considered internally ‘missing’ or when time has elapsed for Data Protection Act, Access to Records, FOI requests etc. requests.

A ‘stolen’ record describes the physical theft of health record/s from the Trust

Refer to the Misplaced Records Procedure CPG9e
5.0 FILING PAPER RECORDS

Filing Original Paper Records:-

5.1 Please note that this procedure only applies to original paper records. This means evidential records that are received in paper format or are records because they have been stamped, sealed, signed or otherwise annotated. Paper documents that are purely photocopied or printed duplicates are not original records. Place only the master copy of a record on file. Extra copies can be made when necessary. Weed out and destroy low-value, non-record information rather than filing it.

5.2 Always consider whether a paper filing system is really needed. Always try to file documents electronically, unless for practical or legal reasons there is the need to maintain paper files. The Trust provides a support facility for the EDRM system to support all users using the electronic document records management system.

Paper Filing Practices:-

5.3 Fundamentally, paper records should be filed in a secure and environmentally safe filing system, which makes best use of space and meets Health & Safety requirements. Ideally each Department should have a central, shared paper filing system in place.

5.4 Files themselves should be grouped in a logical structure to enable the quick and efficient filing and retrieval of information when required and enable implementation of authorised disposal arrangements, i.e. transfer to an archival institution or destruction.

5.5 It is important to arrange files so as not to have conflicting retentions within them and so that security considerations are addressed. For example, this is relevant for Data Protection legislation, as it requires the protection and prompt disposal of personal data. You should therefore establish separate files or file parts for record types with different retention periods and/or confidential information.

(Refer to Appendix C for further guidance on the do’s and don’ts for paper filing practices.)

File Register and Cover Sheet:-

5.6 The existence of all files containing original records must be recorded in a log/register. This register must be used to track the creation, borrowing, movement, archiving or transfer of files, as well as their ultimate disposal. It must allocate a unique identifier (number or alphabetical prefix) to each item / file.

5.7 The file register must be electronic, for example in the use of a spreadsheet or database. The register would contain details such as:

- Department/Team
- File ID
• File Title
• Volume Number
• Room/cabinet location
• Date file opened
• Security constraints on file access
• Date of file closure
• Name and contact details of borrower
• Dates borrowed, expected date for return
• Reason from removing the file
• Special instructions on return (i.e. forward to another source)
• Date file returned
• Date of file closure
• Date and location of archive to a non-office storage location, with any
  archive box number
• Disposal review date (based on appropriate rule within the Trust’s
  retention schedule)
• Disposal Date
• Disposal Action (destroyed or transferred)
• Disposal Authority

This list is not exhaustive....

5.8 In applying retention staff have both the retention period (e.g. 6 years) and
the ‘trigger’ for that period to begin. The ‘trigger’ could be the date the
document was created, the year end in which the document was created, the
expiry or termination of a contract, the completion of a project etc. Staff need
to note that some document types are to be preserved indefinitely or
transferred to The National Archives / Local Archive. Please consult either the
Head of Electronic Systems/Records or Records Manager.

5.9 If a dual electronic and paper filing system is maintained for the same records,
then a note should be made of the existence and location of the electronic
counterparts.

5.10 Every file will need a cover sheet of key information - this is typically attached
to the inside cover. The file cover sheet would have information such as the:

• File reference / ID
• File title/name
• Volume number (with any reference to a continuation volume)
• Filing location/department (For return)
• Protective mark
• File begins date
• File ends date
• Disposal review date (based on appropriate rule within the Trust’s
  retention schedule)

This list is not exhaustive....
**File Closure:**

5.11 Closing files regularly is key to ensuring that files remain manageable and damage to the records is less likely; it also facilitates the application of disposal processes. After closure, no new papers should be added to it, and it must only be used for reference. Files should be closed when either:

- The file becomes too bulky (over 4cm / 2inch thick);
- The case / project has been completed;
- Papers have not been added to it for two years;
- The contents of the file span more than five years; or
- If appropriate, at the end of the calendar or financial year.
- Files should only be closed in conjunction with retention & destruction guidance

5.12 When a file is closed, this should be clearly marked on the file cover, a reference to the new file marked on the closed file, and a reference to the closed file marked on the new file. Do not begin a new file with a paper referring to another paper that is not on that file.

**File Disposal:**

5.13 Based on the information within your File Register, you should periodically review paper files to see which have reached their Disposal Review date.

5.14 Based on the rules within the retention schedules contained in the Information Governance Alliance Records Management NHS Code of Practice 2015, from which this review date is to be calculated, the records will either be destroyed or transferred. Do note that these are recommended minimum retention times from the Department of Health, although where there is a business need, records may be retained for longer periods. Where this is the case the decision must be justifiable. Each department should conduct an annual records review. No records should be destroyed without managerial approval and that there is no need to retain specific records for any ongoing, planned or envisaged litigation, audit, investigation or open Freedom of Information request.

5.15 When undertaking destruction, all records will be disposed of in a manner suitable to their confidentiality and commercial sensitivity. Paper records should be shredded and disposed of as confidential waste. Nothing should ever be left in ordinary rubbish bins, open skips or where it might be vulnerable to casual retrieval. If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. The procedures within the CP9 Health Records Management Policy and CP9g Storage, Retention and Destruction of Records Procedure should be followed, where appropriate to corporate records.

5.16 Records selected for archival preservation and no longer in regular use by the Trust should be transferred as soon as possible to an archival institution (The National Archives/Local Archive). Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act 1958. Records, which are thought to be worthy of permanent preservation, should be referred to the Head of Electronic Systems/Records or the Records Manager for further review.
### 6.0 ACCESS CONTROL TO EDRM SYSTEM

6.1 New staff must sign up to and abide by the Trust’s security, confidentiality and data protection policies.

6.2 A Network Change Control Form must be completed and signed off by Line Managers authorising access to PC systems and electronic records systems. Emails are now accepted from the line manager.

6.3 Active directory will maintain the users of the EDRM system once the system administrators have activated their account.

### 7.0 FILING ELECTRONIC RECORDS

**Where to file Electronic Records**

7.1 Laserfiche is the corporate Electronic Document and Records Management System (EDRMS) in the South of the Trust. It is being used to support non-health business functions.

7.2 Laserfiche allows the set up hierarchies of folders, like Windows, within which scanned and electronically created documents will be stored. Documents will also be 'indexed' with metadata to allow their profiling, cross-referencing and accurate retrieval. A search for documents can be made via this index metadata as well as their name and actual contents.

7.3 When using Laserfiche, staff will receive training on filing, finding and editing documents.

All electronic (final) records must be filed in Laserfiche, once work in progress is finished and they are finalised (with no further change permitted). Where beneficial, for example in making use of the system’s imaging, search, workflow and version control capabilities, Laserfiche may be used to support work in progress; filing documents from the moment they are received or created.

7.4 Until such time as staff have access to Laserfiche, or where documents like spreadsheets are subject to regular active change, records may be filed in a logical filing structure on the network drive, using network user accounts, with appropriate security access controls applied. This means using shared drives which are secure areas. Electronic records must not be filed or stored on local drives of PCs and laptops (e.g. C:\, My Documents, My Pictures, etc.) or any other removable devices (e.g. USB devices, CD etc.).

**Electronic Filing Practices**

7.5 Paper records can be scanned to Laserfiche and electronically generated records can be saved directly from Word, Excel, Outlook and PowerPoint via the ‘Send to Laserfiche’ facility.
7.6 It is important to arrange folders so as not to have records with conflicting retention periods within them. For example, this is relevant for Data Protection legislation, as it requires the protection and prompt disposal of personal data. Consider having separate folders for these records.

7.7 Keep file names short, but meaningful, using keywords relating to the subject of the document. This includes email, where a descriptive title which accurately reflects the content should be chosen. Limit emails to the one subject. Start a new email if the subject matter changes.

7.8 For documents filed on the network, the Trust requires the use of standard naming conventions, as below. The elements of the name would be used as applicable.
   - **Code:** Any relevant reference code
   - **Date:** YYYYMMDD, YYYYMM, YYYY, YYYY-YYYY
   - **Type:** e.g. Minutes, PID, Letter
   - **Name:** Free text, Max 60, Characters
   - **Status:** DRAFT, FINAL
   - **Version:** v0.1, v1.0, v1.1, v2.0

7.9 Within Laserfiche the version control will be automatic however this can be overridden, by an administrator, where necessary. If staff wish to edit a document, they should use the Laserfiche check out/check in capability - this will lock it to an individual for changes, creating a new version when checking back in. Staff should ensure the addition of a version comment.

*(Please refer to Appendix D for further guidance on the do’s and don’ts for electronic filing practices.)*

**Document Indexing:-**

7.10 Within Laserfiche, store records within a folder and profile them with metadata via an index template. The template might have information such as:
   - Reference ID (e.g. for staff, cases, transactions, projects, suppliers, assets etc.)
   - Project /Job/Contract Names
   - Person Names, including correspondents
   - Relevant Addresses
   - Dates relating to document receipt, dispatch, approval, expiry etc.
   - Document types (e.g. job advert, job application, CV)
   - Free text descriptions
   - Work Status, if applicable
   - Closing of activity, case, project, financial period etc.

*This list is not exhaustive....*

7.11 Documents stored within Laserfiche are assigned indexing field values. This permits their profiling, cross-referencing and retrieval via an index search.
7.12 Index fields are grouped together via templates – a template is typically created for a business activity, comprising the fields that are relevant to this process or file type. Templates are applied to both folders and individually to documents.

7.13 Note that the same field can be used across different templates to enable a wider, cross-system search for related documents.

### 8.0 PRESERVATION OF RECORDS

8.1 Electronic records are much easier to manage in line with the Information Governance Alliance Records Management Code of Practice 2015. Electronic systems can be set to destroy, follow manual prompting or automatically in line with required timescales. For those documents which require permanent preservation the quality of the records will be much better preserved electronically than the traditional paper record to support specific organisational historical data, research, etc.

### 9.0 DOCUMENT SCANNING

9.1 For those staff using the EDRM system appropriate scanning equipment needs to be provided.

9.2 Trust Administration Hubs will have a scanning station with the ability for local administration staff to scan from / to. Where identified smaller individual scanners will be installed.

9.3 Once scanned, files will be kept in secure storage until the required quality assurance checks have been completed and validated (see Quality Assurance Form, Appendix A).

9.4 **Scanning Procedure**

9.4.1 All staff will be fully trained by the system administrators – this will include the preparation of files for scanning practice.

9.4.2 Records will require prepping prior to any scanning process taking place. This means that the following work has to be carried out:

- Removal of any paper clips, staples, etc.
- Removal of any post it notes – where these contain information pertinent to the record they should be placed on a blank sheet of paper and scanned individually with this page inserted immediately after the original on which the note was attached.

9.5 **Committal**

9.5.1 Providing all checks as above have been completed and the scanner is satisfied that the file has been scanned correctly, staff are now in a position to commit / store. Once committed / stored documents cannot be altered or added to. The only exception to this via the administrators who can do limited alterations.
9.6 Quality Assurance

9.6.1 Acceptance

- Where processing has enabled selected removal of images i.e. the blank page delete threshold has been set, check the documents to ensure blank pages have been successfully removed.
- If there is any discrepancy or a problem with the images, as defined below, record the details and complete procedure as detailed below.

9.6.2 Definition of Discrepancies

- Image partially or completely obscured – Image found to have another document attached to it that obscures all or part of one or other of the documents.
- Folded documents – Images with evidence that the original document was folded.
- Partial loss of image – Images with evidence that they have loss data on any paper edge.
- Illegible documents – Images for which the content may be partly or wholly unreadable.

9.6.3 Remedial Action

- In the course of carrying out the defined procedure, should a circumstance as described above occur the following remedial actions would be undertaken.

9.6.4 Image Partially or Completely Obscured

- Where an image is found to have another document attached to it that obscures all or part of one or other of the documents additional documents should be checked using the procedures as described above.
- In the event of discovery of a similar fault or loss of image the entire batch of documents scanned should be re-scanned following the documented procedures for such necessary action.
- In the event of no further recurrence with the extended sample testing the single affected batch or documents should be re-scanned following the documented procedures for such necessary action.

9.6.5 Folded Documents

- Images with evidence that the original document was folded may or may not result in loss of data from the final image.
- Acceptance of under 2% of images with no evidential loss will be accepted but recorded.
- Loss of image data through folding of original documents will be verified against quality of original documentation. Where
documentation is of low or poor quality due to storage or age deterioration or similar condition, acceptance of minimal loss will be made.

- Where loss of data is not defined as above, the single affected file should be re-scanned following the documented procedures for such necessary action.

9.6.6 **Illegible Documents**

- Images for which the content may be partly or wholly unreadable may have been as a consequence of poor or illegible original documentation.
- Where this has been identified the scanning procedure should ensure the inclusion of a statement declaring the document status or use the acknowledgement of such circumstance by the recording of such circumstances in the appropriate documentation.
- Where documents are identified as possibly subject to improvement through re-scan the single affected file or documents (as appropriate) should be re-scanned following the documented procedures for such necessary action.

### 10.0 ELECTRONIC RECORD RETRIEVAL

10.1 Only authorised staff will be provided with access to electronic records, as agreed by the completion of the Network Change Control Form.

10.2 Access controls require the following authorisation for the electronic record systems:

- Laserfiche – via Active Directory

10.3 Exceptions to this for printing requests will be for departments / individuals whose roles may specifically require access to written documentation, for example:

- Legal and Insurance
- Complaints
- Information breach investigations
- Integrated Risk
- PPI
- Freedom of Information
- Directors and Non-Executive Directors

10.4 All staff should be aware that the system produces an electronic audit trail of access to and printing from the system.

10.5 Any electronic record / document which is printed from the system cannot, for any reason, be altered, deleted, added to or in any other way amended. All staff will be required to adhere to this practice and anyone found to have abused this may be investigated under the Trust’s disciplinary policies.
11.0 ELECTRONIC RECORD DISPOSAL

11.1 Records may become eligible for disposal under retention schedules contained in the Records Management Code of Practice. This could be identified by calculating the dates of records within folders stored within a 'closed' or archive area of the folder hierarchy.

11.2 EDRM does provide more advanced Records Management functionality, where retention policies can be applied to folders. Staff can discuss use of this with the Systems Administrator.

11.3 Each department should conduct an annual records review. No records should be destroyed without Managerial approval ensuring that there is no need to retain specific records for any ongoing, planned or envisaged litigation, audit, investigation or open Freedom of Information request.

11.4 Special care must be taken with destruction of electronic records, which can be reconstructed from deleted information. Information can be leaked to outside persons through careless disposal of media, including exchange of media as part of a warranty and/or maintenance agreement. The method of media disposal should be based on the risks associated with the content held on the media.

11.5 Overwriting should ensure all previous information has been removed, but this should be done by authorised staff.

11.6 In some cases there will be more than one copy of a record. For example, there are likely to be back-up copies of records held electronically. A record cannot be considered to have been completely destroyed until all back-up copies have been destroyed, if there is any possibility that the data could be recovered.

11.7 For documents stored on the network, record the decision and destruction action and date in a spreadsheet document or database. Electronic systems will log all disposal actions within its audit trail.

11.8 The procedures within the CP9 Health Records Management Policy and CP9(g) Storage, Retention and Destruction of Records Procedure should always be followed, where appropriate for corporate records.

11.9 Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution (The National Archives/Local Archive). Non-active records should be transferred no later than 20 years from creation of the record, as required by the Public Records Act 1958. Records, which are thought to be worthy of permanent preservation, should be referred to the Trust Records Group for review.
12.0 REFERENCE TO OTHER POLICIES AND PROCEDURES

12.1 When processing records in any capacity reference should be made to any Trust policies relating to records as well as to local and professional guidance.

12.2 Other documentation will include:

- Health Records Management Policy and Procedures (CP9)
- Data Protection Act 2018 and Confidentiality Policy / Procedures
- Information Governance and Security Policy / Procedures
- Information Sharing and Consent Policy / Procedure
- Corporate Records User Guide for Laserfiche Document Management System (NOTE—this will be supplied by the Scanning Team / Laserfiche once training is complete)

*This list is not exhaustive....*

END