Essex Partnership University
NHS Foundation Trust

DATA PROTECTION & CONFIDENTIALITY POLICY

POLICY REFERENCE NUMBER:	CP59
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	3 year review; minor changes
AUTHOR:	Alice Williams
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018; September 2021
LAST REVIEW DATE:	September 2021
NEXT REVIEW DATE:	September 2024
APPROVAL BY IGSSC:	August 2021
RATIFICATION BY QUALITY COMMITTEE:	September 2021
COPYRIGHT	© Essex Partnership University NHS Foundation Trust 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 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.

Services	Applicable	Comments
Trustwide	✓	

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)

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION & CONFIDENTIALITY POLICY

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 RESPONSIBILIES

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 fulfil 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
- 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
- Regulation of Investigatory Powers 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)
- HSG (96)15:E5498 – The NHS IM&T Security Manual (Ensuring Security & Confidentiality in NHS Organisations)
- 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)

END

Essex Partnership University
NHS Foundation Trust

DATA PROTECTION PROCEDURE

POLICY REFERENCE NUMBER:	CPG59a
VERSION NUMBER:	3
KEY CHANGES FROM PREVIOUS VERSION	Three year review
AUTHOR:	Alice Williams, Information Governance Manager
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018
LAST REVIEW DATE:	March 2021
NEXT REVIEW DATE:	March 2024
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE	February 2021
RATIFICATION BY QUALITY COMMITTEE:	March 2021
COPYRIGHT	

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.

Services	Applicable	Comments
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

DATA PROTECTION PROCEDURE

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)

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

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 its 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, Mandatory & Essential 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

Essex Partnership University
NHS Foundation Trust

CONFIDENTIALITY PROCEDURE

PROCEDURE REFERENCE NUMBER:	CPG59b
VERSION NUMBER:	3 (third EPUT version)
KEY CHANGES FROM PREVIOUS VERSION	Three year review: Amendments in 1.2; 2.1.4, 2.1.5, 2.1.8, 2.2.1, various minor amendments elsewhere
AUTHOR:	Alice Williams, Information Governance Manager
CONSULTATION GROUPS:	IGSSC
IMPLEMENTATION DATE:	April 2017
AMENDMENT DATE(S):	March 2018; August 2018; Feb 2021
LAST REVIEW DATE:	March 2021
NEXT REVIEW DATE:	March 2024
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE:	February 2021
RATIFIED BY QUALITY COMMITTEE:	March 2021
COPYRIGHT	

PROCEDURE 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.

Services	**Applicable**	**Comments**
Trustwide	✓	

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

ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

CONFIDENTIALITY PROCEDURE

CONTENTS

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

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 Service users expect that information about them will be treated as confidential and are given that assurance under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018

The Trust has a duty to be fair and use a lawful basis for collection and processing of data, all organisations must also be transparent.

Transparency is an important element of data protection. Staff must make sure service users are informed how their data is used and for what purposes it is shared. There should be 'no surprises' for a patient in terms of how their data is used.

The 'transparency' requirements are set out in full in the Articles 12, 13 and 14 of the GDPR. They include making the following information publicly available:

- who the data controller is and how to contact them
- purpose of the data processing
- the lawful basis for the data processing
- information about the data subjects' rights and how to exercise them
- any third parties with whom the data is shared, including
- any transfers to a country outside the European Economic Area (a 'third country') and the safeguards.

The Trust has a 'privacy notice' and 'fair processing' leaflets to inform our service users of how their information is used. These can be found on both the staff pages and on the public website. Leaflets are also available to be displayed in reception areas.

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 service users, 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, guidance regarding courts or police requests must be sought from the Legal team, Trust Data Protection Officer or the Information Governance Manager.

2.1.5 Any decision to disclose confidential information about a service user's treatment or care should always, in the first instance, be brought to the attention of the service user's responsible healthcare worker. It will be their responsibility to assess whether disclosure of information is in the interests of the patient, and decide whether the patient is able to give informed consent.

Advice should be sought in the first instance for any decision that relates to the disclosure of personal data about a service user to a third party
Whether that disclosure is verbal or written, it should be recorded in the service user healthcare record that consent has been gained and if not the reason why it was not, e.g. capacity.

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 ,the Information Governance 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 information breach and will be dealt with under the Trust's disciplinary rules and procedures.

2.1.8 Disclosure or access to the Trust patient systems for any unlawful reason will be treated under the Trust disciplinary rules and procedures.

This includes:

- Your own record
- Another staff members record
- A family members record
- The records of a service user you are not treating or it is not in your job description to access e.g. for administration purposes.

If you come across the record of someone you know or are acquainted with in the course of your work, you must in the first instance log out of the record and inform your line manager.

2.2 **Requests for Confidential Information**

2.2.1 All requests for confidential information concerning a service user, 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. The Access to records team are the responsible team for patient requests. The Legal team are responsible for staff and corporate requests.

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

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 healthcare worker and / or with advice from the Trust's Caldicot Guardian 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 Input, Snapcomms and Communication "all staff" emails
- 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, Mandatory and Essential Training Policy (HR21).

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).**

3 Regulation of Investigatory Powers Act 2000

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 *E. coli* bacteraemias and *Clostridium difficile* infection in patients aged two years or older that are identified in their institution.

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

9 Mental Capacity Act 2005

This Act is for people with a learning disability. It helps make sure that people who may lack capacity to make decisions on their own get the support they need to make those decisions. Where they are not able to make their own decision, the Mental Capacity Act says a decision must be made that is in their 'best interests'.

10 Public Records Act 1958

This Act allows public records to be retained by a department for a further period if the Secretary of State for Digital, Culture, Media and Sport gives their approval. It sets up the place of deposit system, by which other archives services around the country can be appointed to preserve and provide access to public records.

The National Archives' duties under this Act includes -

- provide guidance and supervision to public record bodies on the safekeeping and selection of public records
- preserve transferred records
- provide facilities for the public to see and obtain copies of transferred records, unless the records are withheld because an exemption in the Freedom of Information Act applies.
- oversee the place of deposit system on behalf of the Secretary of State for Digital, Culture, Media and Sport
- return records temporarily at the request of the transferring organisation

Glossary

Patient Identifiable Information	Key identifiable information includes: • Patient's name, address, full postcode, date of birth • Pictures, photographs, videos, audio-tapes or other images (including digital) • NHS Number and local patient identifiable codes • 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.
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.
Implied Consent	This means patients agreement that has been signalled by the behaviour of an informed patient.

Common Law Duty of Confidentiality	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.
Disclosure	This is the divulging or provision of access to data.
Healthcare Purposes	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.
Information Sharing Protocols	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.
Medical Purposes	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 & Social care Act 2001 explicitly broadened the definition to include social care.
Public Interest	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.
Social Care	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).

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 27 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				

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
United Kingdom (EU Exit)				

As of yet, the **United States** does not have any centralized, formal **legislation** at the federal level regarding this issue, and state legislation varies. Any transfer of data to the US must be risk assessed.

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.