

Data Protection and Information Sharing Policy:

(incorporating Confidentiality, Information Sharing, Safe Haven and Pseudonymisation procedures)

This policy outlines how the Trust will meet its obligations under Data Protection Legislation, taking account of confidentiality and the Caldicott Principles.

| | | |
|--|--|-------------------|
| Key Words: | Data Protection, Caldicott, Confidentiality, Information Sharing | |
| Version: | 4 | |
| Adopted by: | Trust Policy Committee | |
| Date this version was adopted: | 28 October 2021 | |
| Name of Author: | Head of Data Privacy/Data Protection Officer | |
| Name of responsible Committee: | Data Privacy Committee | |
| Please state if there is a reason for not publishing on website: | N/A | |
| Date issued for publication: | October 2021 | |
| Review date: | March 2024 | |
| Expiry date: | 1 October 2024 | |
| Target audience: | All Staff including Bank, Agency, Contractors and Locums | |
| Type of Policy | Clinical √ | Non Clinical √ |
| Which Relevant CQC Fundamental Standards? | Regulation 17: Good Governance | |

Contents Page

| | | |
|-------------|---|----|
| | Version Control | 4 |
| | Equality Statement | 4 |
| | Due Regard | 4 |
| | Definitions | 5 |
| 1.0 | Purpose | 7 |
| 2.0 | Summary | 8 |
| 3.0 | Introduction | 9 |
| 4.0 | Duties within the Organisation | 9 |
| 5.0 | General Principles | 12 |
| 5.1 | Legislation, Regulations and Guidance | 12 |
| 5.2 | The General Data Protection Regulation (EU) 2016/679 – Principles and Practice to ensure compliance | 13 |
| | 5.2.1 Processed lawfully, fairly and in a transparent manner | 13 |
| | 5.2.2 collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes | 14 |
| | 5.2.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed | 14 |
| | 5.2.4 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 | 14 |
| | 5.2.5 kept in a form which permits identification of data subjects for no longer than necessary | 15 |
| | 5.2.6 processed in a manner that ensures appropriate security | 15 |
| | 5.2.7 Accountability principle | 15 |
| 5.3 | Caldicott Principles | 16 |
| 5.4 | Confidentiality | 17 |
| | 5.4.1 Patient Confidentiality | 18 |
| | 5.4.2 Staff maintaining Confidentiality | 18 |
| 5.5 | Information Sharing | 19 |
| 6.0 | General Computer/System Security | 20 |
| 6.1 | General Security Measures | 21 |
| 7.0 | The Collection, Use and Sharing of Information | 22 |
| 7.1 | Information for service users | 22 |
| 7.2 | Information about Children and Young People | 21 |
| 7.3 | Information about Individuals Lacking Capacity | 22 |
| 7.4 | Information for Staff | 22 |
| 8.0 | Images, Audio and Video – Clinical and Non-Clinical Use | 23 |
| 8.1 | Clinical Purposes | 23 |
| 8.2 | Clinical Images for Non-Clinical Purposes | 23 |
| 8.3 | Media and Other Promotional Use | 24 |
| 8.4 | Personal Photographs | 25 |
| 9.0 | Information Sharing | 25 |
| 9.1 | Principles of Information Sharing | 25 |
| 9.2 | Information Sharing for Care Purposes | 26 |
| 9.3 | Information Sharing Agreements/Protocols/Contracts | 27 |
| 9.4 | Disclosure of Information to the Police | 27 |
| 9.5 | International Data Transfers | 28 |
| 9.6 | Freedom of Information (FOI) Requests | 28 |
| 10.0 | Safe Haven Procedures | 28 |
| 10.1 | What is a ‘Safe Haven’? | 29 |

| | | |
|-------------------|--|-----------|
| 10.2 | Emails/Electronic Information | 29 |
| 10.3 | Removable Media (USB Sticks/CDs/DVDs etc) | 30 |
| 10.4 | Faxing | 30 |
| 10.5 | Mailing/Posting/Courier | 31 |
| 10.6 | Telephones/ Answer Machines/ Messages/ Verbal Conversations | 32 |
| 10.7 | Whiteboard and other visual aids | 34 |
| 10.8 | Remote Working (Home, Off-site, Community, etc) | 34 |
| 11.0 | Using Information for Training, Research and Audit Purposes | 34 |
| 11.1 | Students, Trainees and Honorary Placements | 35 |
| 11.2 | Training and Education | 35 |
| 11.3 | Research and Clinical Audits | 35 |
| 12.0 | Using Information for System Testing and Training | 35 |
| 13.0 | Pseudonymisation and Anonymisation | 36 |
| 13.1 | Anonymisation | 36 |
| 13.2 | Risk of Re-identification | 36 |
| 13.3 | Secondary Uses of Service User Information | 37 |
| 14.0 | Data Protection Impact Assessments | 38 |
| 15.0 | Confidentiality Audit Approach | 38 |
| 15.1 | Confidentiality Audits | 39 |
| 16.0 | Training Needs | 39 |
| 17.0 | Monitoring Compliance and Effectiveness | 40 |
| 17.1 | Additional Compliance | 40 |
| 18.0 | Standards/Performance Indicators | 41 |
| 19.0 | References and Bibliography | 41 |
| 20.0 | Trust Data Security and Privacy Policies | 41 |
| | APPENDICES | |
| Appendix 1 | Training Requirements | 42 |
| Appendix 2 | NHS Constitution | 43 |
| Appendix 3 | Stakeholders and Consultation | 44 |
| Appendix 4 | Due Regard Screening | 45 |
| Appendix 5 | Privacy Impact Assessment Screening | 47 |
| Appendix 6 | GDPR Processing Conditions for Personal Information | 48 |

| Version number | Date | Comments (description change and amendments) |
|-----------------------|-------------|---|
| | 12 May 2014 | Full Review and reconstitution of the Trust Data |

| | | |
|-----------|-------------------|---|
| 1.0 Draft | | Protection Policy to incorporate Caldicott 2 Review response and in response to incidents/lessons learnt |
| 1.0 | 10 Nov 2014 | Changes following consultation |
| 1.0 | 20/12/16 | The current Data Protection Act is going to be superseded in May 2018 by the EU General Data Protection Regulation .This policy will be reviewed at this stage. |
| 2.0 Draft | 17 April 2018 | Revision in light of General Data Protection Regulation (EU) 2016/679 and UK Data Protection Act 2018 (once Royal Assent received), National Data Guardian report on Data Security, Consent and Opt-Outs; merge with Information Sharing Policy |
| 3 | 03 September 2021 | Revisions in light of Brexit changing GDPR to UK GDPR, including the Accountability principle under DPA 18 and revisions to Caldicott Principles as part of scheduled review |

For further information contact:

Head of Data Privacy/Data Protection Officer

Email: lpt.dataprivacy@nhs.net

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- **Strategies, policies and services are free from discrimination;**
- **LPT complies with current equality legislation;**
- **Due regard is given to equality in decision making and subsequent processes;**
- **Opportunities for promoting equality are identified.**

Please refer to due regard assessment (Appendix 4) of this policy.

Definitions that apply to this Policy

| | |
|---|---|
| Access to Health Records Act 1990 | Provides controls on the management and disclosure of health records for deceased patients. Thus the personal representative of the deceased or a person who might have a claim arising from the patient's death can apply to request access to the records. |
| Caldicott Report | <p>Provides guidance to the NHS on the use and protection of personal confidential information (PCD), and emphasises the need for controls over the availability and access to such information. It made a series of recommendations which led to the requirement for all NHS organisations to appoint a Caldicott Guardian, who is responsible ensuring compliance with the 6 (original) Caldicott confidentiality principles.</p> <p>A review of the Caldicott Principles through a 2012 review by Dame Fiona Caldicott – report “The Information Governance Review – To share or not to share” published in April 2013 added a new Principle.</p> |
| Common Law Duty of Confidentiality | Prohibits the use and disclosure of information provided in confidence, unless there is a statutory requirement or court order to do so. Such information may be disclosed only for the purposes that the individual has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example to protect the vital interests of the individual or another person, or for the prevention or detection of a serious crime |
| Databases | <p>Are any collections of personal information that can be processed by automated means. A few examples are detailed below:</p> <ul style="list-style-type: none"> • Patient/personal records (names and addresses etc) for appointments • Patient/personal information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this can be an Excel spreadsheet • Patient/personal details used for prescribing drugs • Staff records held on Excel or other locally developed databases, to monitor annual leave and sickness <p>Information collected from individuals should be and should all be justified as being required for the purpose they are being requested.</p> |
| Data Controller | Is the body/organisation and/or individual person who controls how the personal data shall be processed. The data controller can be either an organisation, a group of people who share control or an individual member of staff. |
| Data | Under GDPR this is defined as: |

| | |
|------------------------------|---|
| Processing | <i>Any operation or set of operations which is performed on personal data or on data sets of personal data, whether or not by automated means, such as : collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use , disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2))</i> |
| Data Subject | Is the individual to whom the personal data relates. |
| Disclosure | The passing of information from the Data Controller to another organisation / individual |
| | |
| Personal Data | Is information about a living, identifiable individual. This will include any opinion expressed about an individual. It need not be particularly sensitive information, and can be as little as a name and address. |
| Primary uses | Information used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare services provided |
| Safe Haven | Term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure personal confidential information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post, email, telephone or other means. Any members of staff handling confidential information must adhere to safe haven principles. |
| Special Category Data | Under GDPR this is defined as: a) <i>The racial or ethnic origin of the data subject</i> b) <i>His political opinions</i> c) <i>Her religious or philosophical beliefs</i> d) <i>Whether he is a member of a trade union</i> e) <i>Genetic data (for the purpose of identifying a unique person)</i> f) <i>Biometric data (for the purpose of identifying a unique person)</i> g) <i>Data concerning her health; or</i> h) <i>Data concerning a natural person's sex life or sexual orientation</i> (Article 9(1)) |
| Secondary uses | For non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When personal confidential data is used for secondary purposes this |

| | |
|--|--|
| | should, where appropriate, be limited and de-identified so that the secondary use process is confidential. |
| UK GDPR (the Retained (EU) General Data Protection Regulation 2016/679) | Provides controls on the handling of personal identifiable information for all living individuals. Central to the Regulations are compliance with the principles, designed to protect the rights of individuals about whom personal data is processed |

1.0. Purpose of the Policy

The purpose of this policy is to provide the framework that all managers and staff are aware of and comply with in relation to the Trust's statutory obligations and responsibilities, including those under Data Protection Privacy Law (UK General Data Protection Regulation & Data Protection Act 2018), Caldicott Principles and the NHS Code of Confidentiality.

This policy provides guidance on the rights of individuals under the Common Law Duty of Confidentiality and other legislation as appropriate, and outlines the arrangements adopted by the Trust for the auditing and monitoring of confidentiality and data protection within the organisation.

This policy aims to provide clear and robust information sharing procedures to ensure that the Trust is designated as a 'Safe Haven' and meets national standards regarding the receipt and transfer of information. This policy includes guidance on the use of patient information for clinical training, research and systems testing and provides an understanding and procedure for the different means of communication personal and confidential information

This policy ensures that external partner organisations are fully confident that any personal and confidential information released to the Trust will be protected and processed in accordance with any associated information sharing agreements

The Trust, and individual members of staff, have a legal obligation to comply with all appropriate legislation in respect of information handling, information security and confidentiality. This policy does not allege to cover all situations; therefore responsibility lies with staff/departments/services to ensure that the confidentiality/security of information is maintained whilst under their ownership and seek advice from senior management or the Data Privacy Department as necessary.

This policy covers all identifiable information processed about living individuals, (which includes both patients and staff). This includes, but is not limited to:

- Storage, filing and record systems – paper and electronic
- Transmission of information – email, post, telephone and fax
- Images including CCTV and photographs
- Data held in offsite archive storage
- Data held on CD's/DVD's, memory sticks, laptops, tablets, smartphones

and all other types of mobile media

Throughout this document the term “service user” is used to refer to an individual who is receiving a service from the Trust, and this term includes those people who are also known as “patients”, and “Clients”. Similarly the terms “clinician” and “healthcare professional” are used, but should be interpreted as encompassing social care staff and NHS practitioners.

2.0. Summary and Key Points

Data Protection and Confidentiality are legal requirements on all staff working for the Trust.

The General Data Protection Regulation (EU) 2016/679 came into full effect on 25 May 2018. As the UK left the EU in January 2021, this was enshrined in UK law as ‘the Retained General Data Protection Regulation (EU) 2016/679 – UK GDPR and supported by the Data Protection Act 2018. This policy details how the Trust will comply with its legal obligations under this legislation.

Data Protection legislation is not a barrier to processing and sharing as long as a defined ‘legal basis’ has been defined and recorded. The GDPR brought a new principle of ‘accountability and transparency’. This means that Data Controllers (i.e. the Trust) has to ensure that Data Subjects (our service users and staff) are aware of the processing of their personal data and this information is readily available to them. To achieve this, the Trust public website is updated regularly.

As a public authority, (i.e. the NHS) the Trust does not rely on consent as a legal basis to process service user and staff information. This is covered in more detail in section 5.2 and Appendix 6. However, staff should always consider gaining consent from service users and staff when considering whether to share information, as a balance against the common law duty of confidence. Staff should be aware that consent under common law duty of confidence is not the same as consent as a legal basis for processing and the enhanced requirements for consent under Data Protection legislation do not apply. Consent to share information should be recorded on the service users health record and within their personnel file in respect of staff.

All staff must complete annual Data Security Awareness training (formerly Information Governance Training), which covers Data Protection and Confidentiality.

Staff must respect an individual’s right to confidentiality and it is an abuse of privilege should you access service user or staff information on any system (electronic or paper). This includes accessing your own, family members (including spouses; children; parent etc) friends or acquaintances even if it is considered to be within their role in the organisation.

They should also not remove from site, any service user or staff information without the knowledge or agreement of a senior manager, even if they believe they have informal support to do this. Failure to comply could result in disciplinary action and furthermore, deemed as an offence under Data Protection Law and referred to the Information Commissioners Office for investigation.

If staff require advice or support on any Data Protection or Confidentiality matter, they should contact the Data Privacy Team via lpt.dataprivacy@nhs.net in the first instance, who may escalate the issue to either the Data Protection Officer or Caldicott Guardian.

3.0. Introduction

The Trust needs to collect and use information about people with whom it deals in order to operate. These include current, past and prospective service users, current, past and prospective employees, suppliers, clients/customers, and others with whom it communicates. In addition, it may occasionally be required by law to collect and process certain types of information to comply with the requirements of Government departments for business data.

For the purposes of this policy, the terms 'data' and 'information' are used interchangeably

This policy applies to all employees of the Trust, any staff who are seconded to them, contract and agency, bank or locum staff and volunteers.

All employees are responsible for maintaining patient confidentiality. The duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained, whether directly or indirectly, in the course of duty is a disciplinary offence, which could result in dismissal and/or prosecution.

4.0 Duties within the Organisation

4.1 **The Trust Board** has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

4.2. The **Chief Executive** has a duty to ensure that:

- Staff are aware of the need to comply with the Data Protection Law, in particular with the rights of patients wishing to access personal information and/or their health records
- Staff are aware of the requirements of the common law duty of confidence as set out in the Confidentiality: NHS Code of Practice
- Arrangements with third parties who access personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality
- Local Research Ethics Committees and researchers are aware of the Data Protection law and how it applies to the use of data for research purposes.

4.3 **The Caldicott Guardian** (Medical Director) has specific responsibility for reflecting service users interests regarding the use of personal data. They are also responsible for ensuring that personal data is shared in an appropriate and secure manner. To assist with the volume and diversity of this task the Caldicott Guardian is supported by the Head of Data Privacy/Data Protection Officer, Directorate Clinical Governance Leads and Information Asset Owners (who act as Data Custodians).

4.4 **The Senior Information Risk Owner (SIRO)** has Board level responsibility for the management of information risk within the Trust and the development and maintenance of Data Privacy practices throughout the Trust to ensure the safety and availability of information assets. The SIRO is also the Director with responsibility for data and cyber security.

4.5 Under the terms of Data Protection legislation, the Trust must appoint a Data Protection Officer (DPO), who will inform and advise the Trust about its obligations to comply with its legal obligations under data protection legislation, and who will monitor compliance with those legal obligations. **The Head of Data Privacy** has been assigned the role of **DPO** and will manage internal data protection activities, advise on data protection impact assessments, and be the first point of contact for supervisory authorities and individuals whose data is processed.

4.6 **Information Asset Owners** undertake the role and responsibility of Data Custodians, as referred to in the Data Protection Law and are responsible for ensuring that the Data Protection and Caldicott principles are fully observed and complied with by staff within their Directorate/Service/Department. Working with Team/Service Managers, Information Asset Owners are required to ensure that all data flows and processing of data complies with all current Data Protection policies, working closely with the Head of Data Privacy/Data Protection Officer as appropriate.

- Promote Data Protection and Caldicott Principles on an on-going basis
- Ensure that all staff know the procedure for reporting IG and IT security incidents
- Ensure that an annual review of the Information Asset Register is undertaken through delegated responsibility, to enable an assessment of compliance with Data Protection and Caldicott Principles
- Have systems in place to enable the above to be managed effectively within the service

4.7 **Information Asset Administrators** are responsible for supporting Information Asset Owners in ensuring the accuracy, security and lawful use of personal data within their own areas.

4.8 **Managers** will ensure that all staff:

- are aware of the Data Protection Policy and updates in regard to any changes in the Policy,
- undertake appropriate training including the annual mandatory Data Security Awareness Training
- have access to all relevant systems and procedures to support the Policy,
- know how to deal with requests for personal/patient identifiable information,
- know how to access and store personal/patient identifiable information, both manual and electronic records,
- Report actual and potential breaches and issues and seek advice where necessary
- register databases with the Information Management and Technology Delivery Group via their Directorate representative, who will maintain a log of databases and nominated application/system managers

- Undertake annual reviews of data processing activities and notify the Head of Data Privacy of any changes

4.9 **All staff** must be aware of the underlying principle 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.

Staff who become patients do not have an automatic right to view their own information. It is an abuse of privilege for staff to view or access information about their family, friends or work colleagues. Where staff are seeking access to any information held about them in their capacity as an employee or as a patient, a Subject Access Request must be made in line with the Trusts' Individual Information Rights Policy.

Staff whose duties require them to have access to patient information will receive specific guidance and instruction from their direct line manager. Staff need to be aware that inappropriate use or loss of information is a potentially serious and reportable incident, and should be reported in accordance with the Trust Incident Reporting Policy.

All staff are required to sign appropriate data protection and confidentiality clauses to cover their work within the Trust:

- All contracted staff (substantive, permanent, fixed-term, bank, etc) are issued with a contract of employment, and non-medical staff receive a copy of the 'Statement of Main Terms and Conditions', both of which include appropriate data protection and confidentiality clauses.
- All non-contracted staff (agency, volunteers, student placements, suppliers, etc) must be engaged under an appropriate contract which contains clauses to ensure that those staff are bound by the same data privacy rules as Trust staff. Non-contracted staff (all workers without a contract of employment with the Trust), must also sign a Data Security Statement on commencing work with the Trust.

To ensure that staff are effectively informed about what is required of them in relation to data protection, confidentiality and information sharing, this policy has been produced to identify the legal requirements and provide an understanding of what the Trust requires staff to do to keep personal information safe and secure. This policy is highlighted during the Trusts' induction programme, within all data privacy training sessions and materials, and should be covered by line managers during local induction.

All staff are expected to:

- adhere to this Policy and all related systems and processes to implement the Regulation and Act,
- undertake training as appropriate, including their annual Data Security Awareness training (formerly information governance training)

- ensure that all patient/personal identifiable information is accurate, relevant, up to date and used appropriately, both electronic and manual including the use of databases,
- ensure that all patient/personal identifiable information is kept secure at all times.
- ensure that patient information is recorded accurately
- inform patients how their information will be used and ensure that they understand. The patient should understand that the information given will be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided.
- provide choice and allow patients to decide whether their information can be recorded, disclosed or used in particular ways. People have very different needs and values – they must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information.
- improve ways and always look for better ways to safeguard information
- be aware of the issues surrounding confidentiality, and seeking training or support where uncertain in order to deal with patients' information appropriately.
- report possible breaches or risks of breaches to patient confidentiality.

Failure to comply with data protection legislation can lead to enforcement action from the Information Commissioners Office (ICO), including monetary penalties, claims for compensation and/or criminal prosecution. It is the responsibility of every individual member of staff to be familiar with this policy (and all related policies) to ensure the confidentiality, security and integrity of information is maintained whilst under their ownership. Any failure by a member of staff to follow the processes outlined in this policy may result in initiation of the Trusts' Disciplinary Procedure.

4.10 The Data Privacy Committee is chaired by the SIRO and is the forum responsible for ensuring that the Trust embeds a culture of data privacy and co-ordinates the work associated with the data protection and security framework.

5.0 General Principles

5.1 Legislation, Regulations and Guidance

The Trust's Data Protection Officer is the Head of Data Privacy. The Trust has an obligation as a Data Controller to notify the Information Commissioner's Office (ICO) of the purposes for which it processes personal data. The Trust's ICO Registration Number is Z6769559

<https://ico.org.uk/ESDWebPages/Entry/Z6769559>

The Data Protection Act (DPA) is the main piece of UK legislation which governs the use of personal data which identify living individuals. The General Data Protection Regulation (EU) 2016/679 came into effect on 25 May 2018 and replaced the 1995 data protection directive which originated the DPA. As the UK left the EU in January

2021, the GDPR was enshrined in UK law as the Retained General Data Protection Regulation (EU) 2021/679 – UKGDPR, supported by the Data Protection Act 2018. This policy has been revised to reflect the Trust's obligations under Data Protection Legislation as applied in the UK.

There are other rules and regulations which specify how information should be handled. These include, but are not limited to:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1998
- Code of Practice on Confidential Information 2014
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Confidentiality NHS Code of Practice
- Crime and Disorder Act 1998
- Criminal Justice and Immigration Act 2008
- Freedom of Information Act 2000
- HMG: Information Sharing by Practitioners in Safeguarding Services
- Human Rights Act 1998 (Article 8)
- Information Security NHS Code of Practice
- International Information Security Standard: ISO/IEC27002:2005
- NHS Care Record Guarantee for England
- Mental Capacity Act 2005
- Records Management Code of Practice 2016
- Regulations and Investigatory Powers Act 2000
- Social Care Record Guarantee for England

5.2 The UK General Data Protection Regulation– Principles and Practice to ensure compliance

The UKGDPR specifies that the trust “shall be responsible for, and be able to demonstrate, compliance” with these principles which are summary below. The Trust will put in place procedures to ensure the principles in the UK GDPR and UK Data Protection Act are met:

5.2.1

(a) Processed lawfully, fairly and in a transparent manner

Compliance will be achieved by implementing the following measures:

- Ensuring that the Trust's Privacy Notice (available on the Trust website) is kept up to date, and complies with the Information Commissioners Office (ICO) Code of Practice.
- The Trust must have an appointed Data Protection Officer, whose contact details are available to the public
- Complying with the common law duty of confidentiality: that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual

- Ensuring that the legal basis for processing of information is identified, via the recording of processing activities
- Informing the individual how their information will be processed. This means fully describing how the information will be used i.e. what will be done with the information; for what reason will it be used; who will it be passed on to; how will it get there, stored and destroyed

Under the UKGDPR, data subjects have certain rights, which must be upheld:

- Be informed – through privacy notices and the publication of Data Protection Impact Assessments
- Access – Subject Access Requests (please refer to the Trust policy on Individuals Rights)

5.2.2

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose Limitation)

This will be achieved by:

- Completion of Data Protection Impact Assessment where there are changes to the way that information is processed, including the procurement of new systems, use of technology to support clinical practice
- Annual reviews of information flow mapping
- Protocols should be in place to ensure that personal data that is shared is only used for the purposes for which it was originally obtained
- Those involved in research must develop procedures for making patients aware that their information may sometimes be used for research, and explaining the reasons and safeguards. Any objections from patients must be respected (*MRC Executive Summary – Personal Information in Medical Research*)

5.2.3

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

This will be achieved by:

- Conducting routine audits as part of good data management practices
- Ensuring that relevant records management policies and professional guidelines i.e. information lifecycle, are adhered to

5.2.4

(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 (Accuracy)

This will be achieved by:

- Data users recording information accurately and taking reasonable steps to check the accuracy of information they receive from data subjects or anyone else
- Data users regularly checking all systems to destroy out-of-date information and correcting inaccurate information

5.2.5 (e) kept in a form which permits identification of data subjects for no longer than necessary
(Storage limitation)

This will be achieved by:

- Adherence to Data Privacy and Records related Policies (i.e information lifecycle)
- Staff working in joint team situations using the maximum retention period
- Compliance with the Records Management Code of Practice for Health and Social Care 2016 comprehensive retention schedule, which is reflected in the information lifecycle and records management policy

5.2.6 (f) processed in a manner that ensures appropriate security (Integrity and confidentiality – Security)

This will be achieved by:

- Compliance with the Information Security Policies Parts 1 & 2
- Completion of Data Protection Impact Assessments (refer to the Data Protection Impact Assessment Policy and Procedure)
- Appropriate technical and organisational measures shall be taken to prevent the unauthorised or unlawful processing of personal data and against accidental loss or destruction
- Compliance with protocols regarding the transfer of personal data outside of European Economic Area unless that country can ensure an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

5.2.7 The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 ('accountability')

This principle requires the Trust and all its employees to take responsibility for what we do with personal data and how we comply with the other principles (set out above).

Appropriate measures and records are required to be in place to demonstrate the Trusts compliance.

ALL STAFF HAVE A LEGAL DUTY TO PROTECT THE PRIVACY OF INFORMATION ABOUT INDIVIDUALS

5.2.8 All data breaches, incidents and near-misses must be reported via the incident reporting process (ulysses) as an e-irf. Where it involves the inappropriate destruction or alteration, loss/theft or unauthorised disclosure/access to personal or confidential information, the Data Privacy Department must be informed immediately to assess the severity of the breach and support with identifying the remedial action required. Every incident must be reviewed to establish if it is reportable to the ICO, which must happen **within 72-hours of identification**. Failing to notify the ICO of a breach could result in significant financial consequences. Further information and guidance is available in the Incident Reporting Policy.

5.2.9 The UKGDPR and revised DPA do not include principles relating to individual rights or overseas transfers of personal data (previously covered by principles 6 and 8 of the DPA 1998). However, these areas are separately addressed in other Articles and Chapters of the legislation. Further information regarding individuals' rights can be found in the Trusts' 'Individual Rights Policy'/ Additional guidance regarding overseas transfers is available in Section 9.5 of this Policy.

5.3 Caldicott Principles

The Caldicott Guidelines focus specifically on the protection and processing of personal data within the health and care sectors. The Trust maintains a firm commitment to these principles which are:

- Justify the purpose for using confidential information
- Use confidential information only when it is necessary
- Use the minimum necessary
- Access to personal data should be on a strict need to know basis
- Everyone with access to confidential information should be aware of their responsibilities
- Comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform patients and service users about how their confidential information is used

1 – Justify the Purpose

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

2 – Don't use personal confidential data unless 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)

3 – Use the minimum amount of personal confidential data necessary

- Where the use of personal confidential data is considered to be essential, the

inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as necessary for a given function to be carried out.

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 have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes.

5 – Everyone with access to personal confidential data should be aware of their responsibilities

- The organisation must 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

6 – Understand and comply with the law

- Every use of personal confidential data must be lawful. The Caldicott Guardian, Medical Director, is responsible for ensuring that the organisation complies with legal requirements

7 – The duty to share information for direct care is 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

8 – Inform service users and patients about how their information is used

- A range of steps should be taken to ensure that there are no surprises for patients and service users, so that they have clear expectations about how and why their confidential information is used, and what choices they have about this.

The National Data Guardian's report *Data Security, Consent and Opt-Outs*, published in July 2016, set out ten new standards for data security for the NHS, and made recommendations about how individuals might be better involved in and informed about how their information is shared.

Professional bodies (e.g. Nursing and Midwifery Council (NMC), General Medical Council (GMC) and Health Professionals Council (HPC) provide supplementary advice and guidance for their own disciplines. These guidelines should not conflict with this Policy or legislative requirements.

5.4 Confidentiality

The 'Confidentiality: NHS Code of Practice' was published by the Department of Health following major consultation in 2002/03. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and

regulators. The guidance was drafted and delivered by a working group made up of key representatives from these areas.

The Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. This document uses the term 'staff' as a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

This document:

1. Introduces the concept of confidentiality
2. Describes what a confidential service should look like
3. Provides a high level description of the main legal requirements
4. Recommends a generic decision support tool for sharing/disclosing information
5. Lists examples of particular information disclosure scenarios

The full document can be accessed from

<https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice>

To compliment this document a 'Supplementary Guidance: Public Interest Disclosures published in November 2010 is available for NHS staff in making what are often difficult decisions on whether a breach of confidentiality can be justified in the public interest

[https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200147/Confidentiality -
_NHS Code of Practice Supplementary Guidance on Public Interest Disclosures.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200147/Confidentiality_-_NHS_Code_of_Practice_Supplementary_Guidance_on_Public_Interest_Disclosures.pdf)

Following the publication of the Caldicott Review in March 2013, the Health and Social Care Information Centre (HSCIC) published 'A guide to confidentiality in health and social care' which identified five rules for treating confidential information with respect:

Rule 1 – Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2 – Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3 – Information that is shared for the benefit of the community should be anonymised

Rule 4 – An individual's right to object to the sharing of confidential information about them should be respected

Rule 5 – Organisations should put policies, procedures and systems on place to ensure the confidentiality rules are followed

The full document which contains other helpful guidance can be found:

5.4.1 Patient Confidentiality

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

On admission and/or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, and those they specifically **do not** give permission to receive information. This information must be recorded in the clinical record – either an electronic patient record system or paper health record.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

5.4.2 Staff maintaining Confidentiality

All staff should be aware that it is a condition of their contract with the Trust that under no circumstances should information of a confidential nature be discussed with or passed on to any unauthorised persons at any time, either during the course of their work or outside of the working environment, whilst contracted by the Trust or after the contract has terminated. Staff should be aware that they should not use social media, networking sites or other digital applications to discuss any aspect of their contract, or to give an opinion about service users, colleagues or the organisation. Please refer to the Social Media and Electronic Communications Policy for further information

Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis that the public good would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual concerned and the broader public interest in the provision of a confidential service. For guidance on sharing information with the police, please see Section 9.4 of this Policy. Further advice is also available from the Safeguarding Lead and/or the Data Privacy Department (as appropriate).

5.5 Information Sharing

Information should only be shared if it is appropriate, necessary and acceptable to do so. Staff must be able to confidently identify requesters so that information is only shared with the right people. Only the minimum amount of information necessary should be shared, and should be checked for accuracy before release to avoid errors or duplicates.

All information with external organisations must be governed by an appropriate information sharing agreement or contract, and meet the requirements of the relevant legislation. All information sharing agreements must be registered with the Data Privacy Department, and all data flows should be recorded on the Information Asset Register (see the Information Security and Risk Policy for details).

Information sharing within the Trust should be limited to staff who have a legitimate professional reason to access the information as part of their role within the Trust. Just because they work for the Trust, does not mean that they have an automatic right to access the information.

Information should only be shared via secure and authorised means, where appropriate safeguards are in place to protect the information.


6.0 General Computer/System Security

Staff are personally responsible for maintaining the security of their Trust-issued devices (i.e. computer, laptop, smartphone, tablet etc) and the data contained on it/them, in accordance with the Trusts' Information Security and privacy policies and procedures.

Access to any computer/system must be password protected in line with current IT access rules and policies. Staff must not discuss with unauthorised individuals how any Trust computer or security systems operate, and **must not** share their login details, passwords or smartcards with anyone for any reason.

Computer systems should only be used to access information about individuals where there is a genuine, professional work-related reason to do so. All access to Trust computer systems is monitored and must be justified if challenged. Staff **must not** access the personal or confidential information of colleagues, friends or relatives (etc). Staff **must not** use the Trust's computer systems to look up or update their own information, including past, present or pending medical or employment information – this should be managed formally under the Trusts' Individual Rights Policy.

Computer screens should be out of the general/public view and should not face towards windows/doors, to ensure that personal and confidential data is only available to authorised individuals.

Staff must always log out of any computer system or application when work on it is finished, and ensure that the device itself is locked when not in use. PCs and laptops can be quickly locked using 'Ctrl'+ 'Alt'+ 'Delete'+ 'Enter' or 'L'+  on the keyboard. Mobile devices must be secured away and out of sight.

Information should be held on the Trust's network servers, and not stored on local or external hard drives. Staff must not transfer any patient, staff or Trusts personal or confidential information onto any personally owned (or other non-NHS) computer/electronic equipment or device without express permission, which can only be granted in exceptional circumstances.

All Trust data systems must be logged on the Information Asset Register (IAR) with a named Information Asset Owner (IAO) and Information Asset Administrator (IAA) (if applicable). Further details can be found in the Trust's Information Risk Policy.

All staff have a responsibility to familiarise themselves and comply with the smartcard conditions of use. Members of staff with an NHS smartcard must ensure that:

- The safety and security of the smartcard is maintained;
- They do not permit another person to use the smartcard;
- They do not log into systems or software and then allow another person (whether or not they hold a smartcard) to access that system or software;
- They follow the Trust's policies relating to smartcards

When using templates (i.e. for letters, reports, etc), staff must ensure that they use a 'blank' template; not one that has been created for another service users/client/member of staff, etc. Using templates containing another person's details increases the risk of an error or confidentiality breach occurring.

6.1 General Security Measures

A Trust ID badge should be worn at all times – such as an official staff badge or other Trust-issued visitor or contractor pass. If there is any doubt about an individual's identity, they should be challenged and the necessary evidence obtained as required – staff should be prepared to challenge people entering their work area if they do not recognise someone or if they do not have ID displayed.

Cabinets, rooms and other areas containing personal and/or confidential information should be closed and locked when unattended, as far as is practically possible, and should not be accessible to unauthorised individuals at any time.

Information/files should be kept closed/out of sight/locked away when not in use so that the contents are not seen by unauthorised individuals. Under no circumstances should personal or confidential information be left unattended in public areas where it can be seen, read or removed by others (i.e. reception desks, copier devices). Where possible, staff should adopt a 'clear desk policy' – please see the Information Security and Risk Policy for further details.

Staff must ensure that if information is being transported in any form (whether paper or electronic) it is kept secure at all times. Personal and confidential information should not be stored, transported or transferred without adequate security measures. See Information Lifecycle and Records Management, and Remote Working policies for further guidance on safe haven procedures.

Staff must ensure that confidential conversations cannot be overheard by unauthorised individuals and should not 'gossip' about confidential information. Please refer to Section 5.4 regarding confidentiality and Section 10.6 regarding telephones.

7.0 The Collection, Use and Sharing of Information

The Trust must be able to demonstrate the lawful basis upon which it is processing personal and special category data (See Appendix 6 for the lawful basis).

7.1 Information for service users

The Trust's Privacy Notice for service users explains why data is collected, how and where it will be stored and how it will be used and shared. Service users may also be informed through leaflets, posters, statements in booklets and verbally by healthcare professionals providing care and treatment. Service users should be told how their information is to be used before they are asked to provide it – or as soon as possible after.

Where the processing of personal information is necessary to provide a service user with health or social care or treatment, this is legally permitted under Article 6(1)(d-e) and Article 9 (2)(h) of the UK GDPR. Separate consent is not necessary for this purpose provided that the information is not shared wider than necessary, and that 'need to know' principles are strictly enforced. Staff must also be aware of any duties of confidentiality which apply to the information or the circumstances (see Section 5.4).

The explicit consent of the service users must be obtained before their information is processed for any reasons other than direct provision of health or social care and where it is not covered by any other legal condition in the UK GDPR (See Appendix 6).

7.2 Information about Children and Young People

Where information relates to a child less than 13 years of age and consent is required for lawful processing, this must be obtained from a person with parental responsibility or other legal guardianship for the child. This authority must be verified and documented with the consent.

If the child/young person is aged between 13 and 18 years, it may be lawful to obtain consent directly from the individual; however, this will depend on the information being collected and the reason(s) for the processing. The Trust must be confident that the child/young person is Gillick competent and is capable of understanding the request and providing informed consent. It may still be appropriate to obtain consent from a person with parental/legal responsibility.

7.3 Information about Individuals Lacking Capacity

Where the information relates to an individual who lacks capacity and consent is required for lawful processing, this must be obtained from a person with legal responsibility for the individual – for example, someone with the appropriate power of attorney. This authority must be verified and documented with the consent.

7.4 Information for Staff

As part of its responsibilities as an employer, the trust will collect, process and share information about its staff, which is lawfully permitted under Article 6(1)(e) and Article

9 (2)(b) of the UK GDPR.

The Trusts' Privacy Notice for staff explains why the data is collected, how and where it will be stored and how it will be used and shared. This is referred to within the Main Terms and Conditions which is issued to all staff. The privacy notice is available on the Trust's public website and is included on all job adverts and displayed in key locations.

The personal information of staff, such as name and job role, may also be collected and used by the Trust as part of its duties as a public organisation – for example, as part of meetings or within policies. This is lawfully permitted under Article 6(1)(e) of the UK GDPR.

The explicit consent of staff must be obtained before their information is processed for any reason(s) not covered by any other lawful condition under UK GDPR.

8.0 Images, Audio and Video – Clinical and Non-Clinical Use

Staff must ensure that the authorised use of camera devices and images for all clinical and non-clinical purposes is carried out with due regard for the rights of all service users, staff, visitors and members of the public. The Trust upholds the right of an individual to appropriate care, balanced with privacy and confidentiality.

Staff must not use their personal camera devices to take any type of medical/clinical image for any purpose without explicit permission of their line manager and the Data Privacy Department (which will only be given in exceptional cases). Also refer to the Trusts Staff Mobile Device Policy for further information.

Depending on the purpose (and content) of the image required, written consent may not be required from the individual – see figure 1 below.

Please also refer to the Trust's 'Consent for Treatment' Policy. Additional guidance is available from health professional bodies.

8.1 Clinical Purposes

Images made for clinical purposes form part of a service users health record, and therefore the processing of this information is lawfully permitted under Article 9 (2)(h) of the UK GDPR. Separate consent is not required for this purpose; however, staff should always ensure that service users are aware of the reason(s) for the image, and that it will be retained within their health record. Images obtained for clinical purposes should not be used for any other purpose without explicit consent (see 8.2 below)

8.2 Clinical Images for Non-Clinical Purposes

Clinical images of service users can only be used for non-clinical purposes (such as research and training) with explicit consent from the individual. The only exception to this is if the images are fully anonymised and have no ability to identify the specific individual to whom they relate. Particular care should be taken when an anonymised image may still have the potential to identify an individual (for example, where a

rare condition is clearly visible).

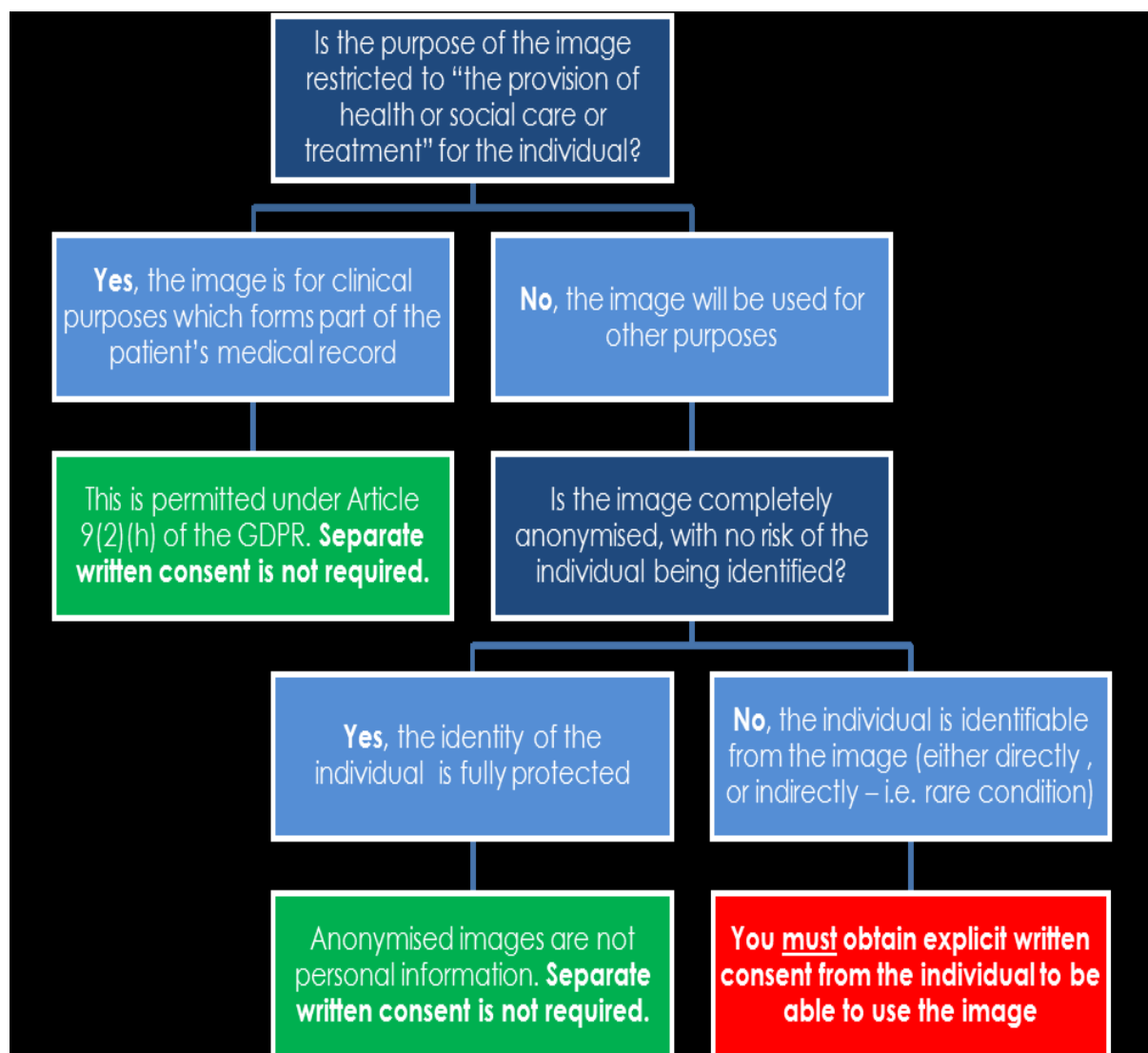


Figure 1

When clinical images of service users are required for non-clinical purposes, the accountability and responsibility for the use of the images rests with the requesting member of staff, as does the requirement to obtain appropriate consent.

The standard images 'Audio and Visual Recordings' consent form should be signed by the service user (or their carer, representative, parent or guardian, as applicable). The signed consent form should be uploaded into the EPR with the images, and a copy given to the signatory. The template consent form is available on the intranet.

8.3 Media and Other Promotional Use

From time to time, the Trust seeks to promote the services that it provides and raise awareness of good-news stories and achievements. This may be through in-house managed platforms, such as newsletters, the public website and social media, or via external organisations such as journalists, broadcasters and in professional or medical journals or publications. Images taken/obtained by the Trust may only be

used for this purpose with the explicit permission of the individual to whom they relate.

The standard images 'Audio and Visual Recordings' consent form should be signed by the individual (or their carer, representative, parent or guardian, applicable). The template consent form is available on the intranet. The signed consent form should be retained by the person taking the image, and a copy given to the signatory. It is the responsibility of the ward/department to manage the storage of the media and relevant consent forms. These must be stored centrally on the network (not local PCs or devices) with appropriate access to relevant staff for audit and reference purposes.

Further guidance on media usage is available on the ICO website:

<https://ico.org.uk/for-organisations/media/>

8.4 Personal Photos

It is appreciated that relatives and visitors of service users may wish to take photos of their loved ones whilst they are in the care of the Trust. In addition to the requirements of the Trust's Social Media and Electronic Communications Policy , there are some conditions for allowing this practice:

- Images should be restricted to non-clinical areas (such as corridors, waiting rooms or outside). Images can only be taken in clinical areas (such as wards and treatment rooms) with the express permission of a senior member of staff i.e. ward matron;
- Consideration should be given to the appropriateness of the image (i.e. the condition or portrayal of the individuals in shot, and their surroundings). If there is any doubt, the request should be discussed with a senior member of staff or the Data Privacy Department;
- Images must be limited to the person/people they are aimed at (such as the service user and their relative) and should not include any other individuals without their explicit permission. Images should not be taken of an unconscious service user without the express permission of a senior member of staff and a justifiable reason for taking the image;
- Images should not be uploaded to social media or other networking sites without explicit permission from all individuals included within the image. Providing consent to have the image taken does not give automatic consent for sharing of the image. If the image has been specifically taken for official medical usage by the Trust, explicit consent is required – please see section 8.3
- If an image has been taken and used inappropriately or without permission, the individual should be asked to permanently delete the image, and provide evidence that this has been actioned. Where deletion/removal is refused, this may result in legal action and/or disciplinary action in the case of staff. Any abuse of images should immediately reported as an incident via ulysses (e-irf).

9.0 Information Sharing

9.1 Principles of Information Sharing

The sharing of any personal or confidential information should be governed by a balance between clear rules which satisfy the requirements of law and guidance, and the encouragement of efficient working practices in both the disclosing and receiving organisations. The Trust will endeavour to have mechanisms in place to ensure that:

- Service users are aware of who the Trust's information sharing partner agencies are (see section 7.1 relating to Privacy Notice);
- Consent is obtained as appropriate (see section 7.1);
- There are regular reviews of information transfers as part of the annual data flow mapping

Individual's rights regarding the sharing of their personal information are supported by the NHS Care Record Guarantee, which sets out high-level commitments for protecting and safeguarding service use information. Particularly in relation to individual's rights of access to their own information, how information will be shared (both internally and externally) and how decisions on sharing information will be made.

The NHS Constitution sets out a series of service user rights and pledges which all NHS organisation are required by law to take into account as part of their decision and actions. This includes an individuals' *"right to privacy and confidentiality, and to expect the NHS to keep [their] confidential information safe and secure"*

The Trust will endeavour to ensure that all information transfers in or out of the organisation are protected by appropriate information sharing agreements and the receipt and transfer of all special category data and Trust confidential information occurs within the boundaries of this policy and associated procedures. Please also refer to the section regarding Safe Haven procedures.

9.2 Information Sharing for Care Purposes

Health and Social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by the Caldicott Principles (see section 5.3). The primary concern must be the health and wellbeing of the individual receiving direct care, and a failure to share information (both efficiently and securely) may have serious consequences for service user welfare.

Where a service user's care or treatment is transferred to another NHS organisation, the record may be transferred directly with the service user themselves (if the transport is co-ordinated by the Trust) or via a request from the other organisation to the Trust's Information Request Team. As the sharing of this information forms part of the service user's ongoing healthcare, this is lawfully permitted under Article 6 (1)(d-e) and Article 9 (2)(h) of the UK GDPR and separate consent is not required. However, the referring clinician must ensure that the service user is aware of the information sharing. Where a service user chooses to seek care or treatment from a private organisation, information will only be shared by the Trust with explicit written permission from the service user. Further guidance is available within the Trust's Individual Information Rights Policy.

Inpatient and community services must ensure that systems are in place to support

coordinated care through clear and accurate information exchange between health and social care professionals, both internal and external to the Trust, as appropriate to the service users ongoing care and treatment/support.

Staff should ensure that systems are in place to establish, respect and review service user preferences for sharing information with partners, family members and/or carers.

9.3 Information Sharing Agreements/Protocols/Contracts

Personal and confidential data may only be shared outside of the Trust where there is a legal justification or explicit consent from the individual concerned. All information sharing with organisations outside of the Trust must be governed by appropriate information sharing agreement, commercial contract, service level agreement or other appropriate legal documentation, which includes data privacy clauses/arrangements. This includes sharing with other NHS organisations, unless the sharing is a direct result of a transfer of, or referral for care.

The Trust is a signatory to the Leicester, Leicestershire and Rutland Strategic Information Sharing Protocol, which provides the overarching principles to encourage the appropriate sharing of information between agencies for the purpose of providing health and social care services to service users. However, this does not overrule the need to have specific information sharing agreements in place where there is information sharing between organisations.

Further guidance regarding information sharing is available from the Data Privacy Department.

9.4 Disclosure of Information to the Police

Data Protection legislation allows for personal data to be disclosed to the police in order to assist in “the prevention or detection of crime” and/or “the apprehension of prosecution of offenders”. Section 115 of the Crime and Disorder Act 1998 also allows the sharing of information to “relevant authorities” (for example: the police, local authorities, health authorities, and local probation boards), “where the disclosure is necessary or expedient for the purposes of any provision” of the Act.

If the individual who is the subject of the request is available and capable, they should be asked to provide their explicit, written consent for the Trust to disclose the information requested, unless this would prejudice the enquiry or court case. For the Trust to consider releasing any information without consent, the request must relate to a serious crime (under the Crime and Disorder Act 1998), otherwise the Police should be asked to obtain a Court Order or written consent.

All requests from the police should be submitted in writing (electronic or hard copy), ideally presented on an official data release form. Requests should be dealt with by the Information Request Team or the Legal Team, depending on the nature and subject of the request.

If there is any doubt about releasing information to the police, advice should be sought from senior management and/or the Data Privacy Department before any

disclosure is made. A copy of the Police request, the decision made and any information supplied must be recorded on the individual's record.

9.5 International data transfers

Restricted transfers to other countries, including to the European Economic Area (EEA) are now subject to transfers under the UK data protection regime. The UK transfers broadly mirror the EU rules, but the UK has the independence to keep the framework under review.

There are provisions which permit the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision'.

Personal data can continue to flow freely between Europe and the UK following agreement by the European Union to adopt 'data adequacy' decisions.

The UK government has the power to make its own 'adequacy decisions' in relation to third countries and international organisations. In the UK regime these are now known as 'adequacy regulations'.

There are also provisions which allow the [continued use of any EU Standard Contractual Clauses \('SCCs'\)](#), valid as at 31 December 2020, both for existing restricted transfers and for new restricted transfers.

Finally, there are provisions which allow certain [Binding Corporate Rules](#) to transition into the UK regime.

For any change to processing, engagement with a new supplier or renewal of a contract, it is important to ascertain if there are any flows of data outside of the UK. These should be included in any Data Protection Impact Assessment and a review of the ICO's International Transfers checklist undertaken to ensure that the appropriate controls are in place including any engagement with the Information Commissioners Office in relation to restricted transfers.

9.6 Freedom of Information (FOI) Requests

Where an organisation is defined as a 'public authority', the Freedom of Information Act 2000 (FOIA) puts a duty on the organisation to provide information to individuals who make a written request for it. There is a list of exemptions which prevent the release of certain information – such as personal and confidential information which identifies individual staff or service users. All FOI requests are coordinated via the Data Privacy Department to ensure that only appropriate information is released and shared. This process is governed under the Trust's Freedom of Information Policy.

10.0 Safe Haven Procedures

We hold large amounts of personal confidential data about our service users and staff. **Staff must ensure that they have done everything possible to protect this information**, and comply with the Caldicott and Data Protection principles.

10.1 What is a 'Safe Haven'?

"Safe Haven" is a virtual concept used to describe an agreed set of arrangements and safeguards that are in place to ensure that personal and confidential information can be communicated safely and securely. The term was originally used to cover the transfer of information by fax, but now it also covers all data held, used and transferred by post, telephone/answerphone, digital and manual records, white/notice board, email and bulk data transfers (51 records or more). Every member of staff is personally responsible for taking precautions to ensure the security of information, using the most up to date, reliable and approved forms of data transfer.

The Trust will endeavour to ensure that all locations on-site where personal or confidential information is received, held or communicated are deemed as safe havens. These designated safe havens will use a combination of measures (physical, electronic and personal) to protect information, and the best practice principles described in this policy should be applied to all incoming and outgoing information flows to ensure that they are secure, justifiable and proportionate.

The clear priority is that members of the public and visitors to the Trust, do not gain access to any area of the Trust deemed as a safe haven. Any physical safe haven locations should be locked or accessible via a coded key pad (or other robust locking mechanism), the code/key for which is only known/accessible to authorised staff; or it should be sited in such a way that only authorised staff can enter. If located on the ground floor, any windows should have locks on them which are used accordingly. The area should conform to health and safety requirements in terms of fire, safety from flood, theft and environmental damage.

The Trust also operates a clear desk policy in order to:

- a) Support the security of personal and confidential information;
- b) Ensure a professional image of the Trust is presented to service users, visitors and other staff; and
- c) Encourage a reduction in the amount of paper used by staff

Scientific studies have also shown that having a clear desk reduces stress, as well as helping to minimise accidents and spills.

At the end of the working day, staff are expected to tidy their desk/workspace and to clear away all hard copy records. Mobile devices should not be left on display or accessible to unauthorised individuals. It may also be appropriate for hard copy records and mobile devices to be put into a locked cabinet/drawer etc. PC's must be switched off, logged out if continued use is required by other authorised individuals.

10.2 Emails/Electronic Information

Personal or confidential information should only be sent via email if it is appropriately secure/encrypted. Only official NHS –issued email account should be used to send or discuss personal or confidential information. Personal/home email addresses should never be used by staff for any Trust business.

Where an email is sent from outside of the Trust to another NHS Mail (@nhs.net) address, this is deemed as secure. However, emails sent to any other address should be manually encrypted by including '[secure]' in the subject line of the email.

Personal and confidential information must not be transmitted via the internet without it being encrypted, or where system-to-system networks are known to be secure. Where online submissions are required, this should be discussed with Leicestershire Health Informatics Service (LHIS) first. Further guidance regarding emails and electronic transfers is available in the Trust's Information Security and Risk Policy.

Dictation machines and devices can contain extremely sensitive information and should always be held securely and kept in a locked area when not in use. They should be cleared of all dictation when the content has been completed/processed.

Where possible, photocopying./scanning machines should be sited in areas away from the general public, and must have the secure-printing function enabled. Care should be taken by staff to ensure that paper is not left on the glass after copying and all printing and copying is collected without delay. Staff must ensure that they have the correct printer selected when sending information to print to avoid confidential or personal information becoming inappropriately available to others.

10.3 Removable Media (USB Sticks/CDs/DVDs etc)

Personal and confidential information should not be stored on removable media unless absolutely necessary. If you have a requirement to use removable media, you should discuss the available options with LHIS.

Where the use of removable media is required and approved:

- a) The information should only be retained on the device for the minimum period possible (the information should be backed-up to networked storage if it is to remain on the device for more than a simple transfer between Trust systems);
- b) Only a Trust-approved device, encrypted to nationally approved standards, should be used (unless authorised by both LHIS and the Data Privacy Departments); and
- c) The physical security of the device must be protected

10.4 Faxing

In support of NHS England's desire to cease "the outdated use of fax machines", the Trust does not encourage faxing as a method of transfer for the same reasons of safety and efficiency.

Personal and confidential information must only be sent by fax where it is absolutely necessary to do so, and there is no alternative method of transfer.

The justification for the continued use of faxes is required in order that the Trust is cited on areas of risk and to determine if there may be more secure means of transferring information i.e. by secure email. A fax checklist is available from either the procurement or health informatics teams, and submitted to the Head of Data Privacy for approval.

Where it is absolutely necessary to send a fax message, this should be sent using the safe haven procedures described below:

- The fax should be sent to a safe haven location where only individuals have a legitimate right to view the information can access it. Confidential faxes, both incoming and outgoing, must not be left where unauthorised people may see them
- Faxes sent must include a cover sheet, which is marked 'Private and Confidential' and contains a suitable confidentiality clause (a template is available on the intranet via the Data Privacy Team pages)
- The sender must be certain that the correct person will receive the fax. The recipient must be notified when the fax is being sent and should be asked to acknowledge receipt. If possible a report sheet should be produced to confirm successful transmission
- Staff should ensure that the fax number is correct and take care when dialling. Where possible, pre-programmed numbers should be used (and regularly checked for changes)
- Only the minimum amount of personal and confidential information should be included in the fax message. Where possible, the information should be anonymised or pseudonymised (see section 13 for more details)

If a document is incorrectly received within the Trust, it is the receiving areas responsibility to ensure that it is given to the named recipient and/or the sender is notified of the error. The error should also be reported via safeguard (e-irf).

10.5 Mailing/Posting/Courier

Care must be taken to ensure that both internal and external mail is addressed correctly and is packaged appropriately.

In public areas, incoming mail should be opened away from public view, stored face down and not left unsupervised.

Envelopes containing personal or confidential information must be securely sealed, addressed to a specific individual and clearly marked "private and confidential" and/or "for addressee only". External mail is automatically marked as sent from the Trust when franked by the post room, indicating a return address if required.

Care should be taken by staff to ensure that envelopes do not contain information which is not intended for the recipient. For example, inadvertently picking up two patient's letters instead of one and sending them to the same address. This can result in a serious breach of confidentiality and could lead to serious consequences for the Trust.

When sending highly sensitive or confidential information, careful consideration should be given to the method of transport and the suitability of the packaging material. When sending by external mail, this must be via a secure method where the package can be traced and is signed for on receipt.

The internal mail should be avoided when sending highly confidential information – this should be hand-delivered where possible. When transporting personal or

confidential information by hand, it must be appropriately secured (for example, placed in a non-transparent envelope or lockable case) to avoid information being lost or inappropriately visible.

Health records or other personal confidential information for transportation between sites/departments must be enclosed in sealed bags/envelopes/boxes and labelled appropriately i.e. 'Confidential', and if relevant, marked 'to be opened by addressee only'. Guidelines for the transporting of health records are available on the intranet, and from the Data Privacy Team via

lpd.dataprivacy@nhs.net

Only companies that hold an existing contract/SLA with the Trust (with appropriate data privacy clauses) can be used to transport service users, staff, equipment or documentation. Any personal or confidential information transported in this way should be signed in and out appropriately and copy evidence of sending/receipt retained. Further advice is available from the Data Privacy Department.

10.6 Telephones/ Answer Machines/ Messages/ Verbal Conversations

Staff are expected to apply common sense with regard to the location used for confidential telephone calls or discussions. For example, using a private office instead of an open plan area, and not playing received answerphone messages on speakerphone in public areas or locations where there is a risk that they could be overheard by unauthorised individuals.

The contact information of individual staff must never be given over the phone unless that member of staff has authorised its release, or it is already within the public domain. This includes Trust email addresses and extension numbers.

When speaking with individuals over the telephone, it is important to confirm their identity before any personal or confidential information is disclosed. Staff must also ensure that the individual has a right to access the information. If the individual's identity cannot be verified and/or the member of staff dealing with the call is uncomfortable with releasing the information over the telephone, no information should be released.

Staff must be aware of the issues surrounding service users whose electronic record has been marked with an alert showing the needs for anonymity or additional safeguards. Any caller wanting information on a flagged service user should be put on hold and immediate advice sought from senior management.

When dealing with incoming calls, staff may need to apply different safeguards depending on the type of information being requested and who the caller claims to be:

- a) Outpatients/Inpatients: Personal information relating to outpatients should only be disclosed to the service user. For inpatients, all calls are directed to the ward/department where the service user is located unless there is an EPR alert preventing this. Therefore, it is imperative that any special circumstances regarding an inpatient's circumstances are appropriately raised and recorded.

- b) The Service User: Before releasing any information to a caller who claims to be a service user, staff should ensure they gain assurance of the caller's identity by obtaining confirmation of certain details, for example: Data of birth, address and post code, appointment dates, treatment/clinic details, hospital or NHS number. A service user may choose to apply an additional safeguard to their health record by insisting that a password they have set up is provided by any caller before any information is released.
- c) Next of Kin: Information should only be disclosed to next of kin, relatives or friends when the consent of the service user has been obtained. It is important to note that next of kin do not have any automatic right to access confidential service user information. Parents/ those with parental responsibility have a right to information about their children, unless the child has sought treatment independently of their parents.
- d) Relatives/Representatives: As part of the admission process, service users may be asked in advance whether they wish for information about their care to be shared with any named individual. Information may then be shared with that individual, either in person or over the phone, without the need to gain further consent. Where a named representative is confirmed, their contact details should be recorded on the service users electronic health record and manual records to ensure their wishes are consistently followed.
- e) Other Third Parties: Where other individuals (e.g. health and social care providers, the police, local authorities, etc) request information about a service user, you must be able to confirm the caller's identity and see evidence that they are authorised to receive the information (such as the service user's consent, legal authorisation etc)

A service user's right to privacy means that when making outgoing calls, we need to speak to the service user directly, unless we have specific consent from them or it is justifiable to speak to someone else. Wherever possible, service user's should be asked in advance if they have any preferences and these should be centrally recorded and regularly checked for updates/changes. For example: Would they prefer to be called at work or home? Would they like information to be left with a family member if they know they cannot be contacted directly? Are they happy for voicemail messages to be left?

When leaving answerphone messages for service users, (only do so with the service users consent) there is a balance to strike between respecting the privacy of the individual, not unduly worrying them with an obscure message, and ensuring that the recipient understands that it is a genuine message (e.g. not a scam that is looking to get them to call back a premium rate number). Staff should take responsibility for considering whether any particular privacy issues exist that could affect whether it is appropriate to leave an answerphone message. For example, staff should consider the following:

- Have the service user's preferences been followed?
- Who else might hear the message?
- Has the correct number been dialled?

- Will the service user fully understand the content of the message?
- Can you be certain the message will be received?
- Is there a risk of breaching the service user's confidentiality?

10.7 Whiteboard and other visual aids

Whiteboards (and similar other visual aids such as notice boards, TV and PC screens) are used all around the Trust to support with the effective delivery of our services. However, when displaying information which may be seen by individuals such as visitors, service users or the general public, it is important that confidentiality is not compromised by displaying too much information.

All service user details (clinical and non-clinical), must be handled in such a way as to remain confidential between the Trust and the service user. As well as having data privacy implications, there are safeguarding issues to consider.

Where a Whiteboard, notice board or other visual aid is used in an area where it is on open view to the public or in a prominent position, it must not be used to display any personal or confidential information where this can be used to identify an individual. Where no other suitable location is available, only the minimum amount of information should be displayed and appropriate safe haven procedures must be in place to protect the information without compromising clinical or service user needs. For example, where boards are used to monitor service user locations/consultants/conditions (etc) on a ward; only use the service user's initials, not their full name; you can indicate that an alert exists for a service user, but not display details of the alert, etc.

These principles also apply to staff information, such as rota and annual leave details – this information should not be on display in public areas, or in a way which makes the information accessible to unauthorised individuals. Where photos of staff are displayed on public notice boards as an introduction to the ward or team, then this is acceptable provided that the individual member of staff have consented to this.

10.8 Remote Working (WFH policy required, Off-site, Community, etc)

Staff are responsible for the confidentiality and security of any information that they hold remotely, either in paper or electronic format, and for its transportation to and from Trust premises. Staff should ensure they hold only the minimum level of confidential information remotely, and ensure compliance with the relevant Information and Data Privacy policies.

For further details and guidance regarding remote working, please refer to the Trust's Information Security and Risk Policy.

11.0 Using Information for Training, Research and Audit Purposes

Additional advice and guidance is also available online via the GMC website:

https://www.gmc-uk.org/guidance/ethical_guidance/30660.asp

11.1 Students, Trainees and Honorary Placements

If a student, trainee or honorary clinician/healthcare provider is included within the healthcare team providing (or supporting) a service user's care, they can have access to the service user's personal information in the same way as other team members, unless the service user objects.

Service user's must be asked to provide their agreement to allow a trainee or student to sit in on any clinical consultation. It is the lead clinician's responsibility to ensure that the service user is under no pressure to agree, and that the trainee/student's presence does not adversely affect the service user's care.

11.2 Training and Education

Most service user's undersand and accept that health education and training relies on having access to information about service users and medical conditions. For most of these purposes, anonymised information will be sufficient and should be used whenever practicable. If information or media is used which can (directly or indirectly) identify an individual, then explicit consent must be obtained.

11.3 Research and Clinical Audits National Data Opt-Out

The Trust will endeavour to ensure that systems of authorisation for research projects are in place and that local ethical and audit committees are aware of the responsibilities of clinical staff and researchers in relation to confidentiality and the promotion of good practice. Further guidance is available through the Research and Development and Clinical Audit Departments.

12.0 Using Information for System Testing and Training

There are a number of risks that exist whenever system testing or training is undertaken using live data or a live environment, including unauthorised access to or disclosure of information and/or corruption or loss of data. These risks can also lead to financial loss to the Trust and/or the person to whom the information relates.

The ICO advises that the use of personal data for system testing/training should be avoided. Where there is no practical alternative to using live data for this purpose, system administrators should develop alternative methods of system testing/training. Before commencing any system testing/training using live data, staff must undertake a Data Protection Impact Assessment (DPIA) - see Data Protection Impact Assessment Policy and Procedure. If the ICO were to receive a complaint about the use of personal data for these reasons, their first question to the Trust would be to ask why no alternative to use the live data had been found and how we documented the risk assessment and decision taken.

For general staff training purposes, live data should not be used as a dataset without explicit consent from the data subject. Fictional, convincing information is the most appropriate dataset to be used, where no real person can be identified from the information used.

Where personal or confidential information has the potential to be used for training

purposes in the future, the individual must be informed at the time of collecting the data and appropriate consent obtained. For example: if telephone calls are recorded for training and monitoring purposes, it may be proportionate to use a recording of a conversation to review how it went, in order to identify training needs with the staff member involved, as long as the data subject has been informed as above. No recording or use of a transcript of a call or conversation may be used for wider training purposes unless we have explicit permission from the data subject – the fact that a person has not objected to the recording itself is not good enough for this purpose.

13.0 Pseudonymisation and Anonymisation

Pseudonymised information is where an individual's identity is disguised by using a unique identifier (a pseudonym). The pseudonym does not reveal an individual's 'real world' identity, but allows the linking of different data sets for the individual concerned. Pseudonymised data is still classed as identifiable data and should be handled as such and must only be transferred using secure means.

13.1 Anonymisation

Anonymised information does not identify an individual and cannot be reasonably used to determine their identity. Anonymisation requires the removal of any detail, or combination of details, that might enable identification, either by itself or when used with other available information.

Effectively anonymised information (where the prospect of identifying individuals is remote), is not seen as personal data and therefore data protection rules do not apply.

It is generally acceptable for anonymised information to be used or disclosed without the data subject's consent, as the information can no longer be used to identify a specific individual. However, the anonymization must be done effectively (see ICO Anonymisation Code of Practice), and neither the anonymization process, nor the use of the anonymised information, should have any direct detrimental effect on any particular individual.

13.2 Risk of Re-identification

To ensure that effective pseudonymisation or anonymization has been applied, a 'motivated intruder' test should be undertaken. This checks whether a reasonably competent individual who wished to de-anonymise data could successfully do so. Further guidance on conducting this test and the steps to follow is available within the ICO Anonymisation Code of Practice:

<https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/>

There are cases where it will be difficult to determine whether there is a reasonable likelihood of re-identification taking place. For example: it is difficult to determine the risk of re-identification of pseudonymised data sets, because even though pseudonymised information does not identify individuals to those who do not have access to the 'key', the possibility of linking several pseudonymised datasets to the

same individual can be a precursor to identification. Any concerns should be discussed with the Data Privacy Department before any information is released.

13.3 Secondary Uses of Service User Information

Service User information is collected for the purpose of delivering health and care services to the individual. This is known as 'primary use' (or direct healthcare purposes), and also includes relevant supporting administrative processes and audit/assurance of the quality of services provided. 'Secondary use' refers to the use of service user information for non-direct healthcare purposes, such as research, audits, commissioning and reporting.

The principles of pseudonymisation and anonymization apply to the use of service user information for secondary use. Through de-identification, users are able to make use of individual data for a range of secondary purposes without having to access the identifiable data items.

Staff must only have access to the data that is necessary for the completion of the business activity they are involved in. This is reflected in the Caldicott Principles ('need to know' access) and extends to both primary and secondary uses.

For direct healthcare purposes, the use of identifiable data is required to ensure patient safety. Under data protection legislation, the Trust is permitted to use service user information for the purposes of preventative or occupational medicine, medical diagnosis, the provision of health or social care systems and services. The use of identifiable service user data for secondary purposes must have a legal justification and/or explicit written consent:

- a) A number of non-direct healthcare purposes will routinely be conducted with explicit service user consent. For example: consent for staff to access information for the purpose of investigating a complaint, or consent for a third party (solicitor, other family members etc) to be given access to data as part of a subject access request.
- b) Existing legislation provides support for a number of non-direct healthcare purposes. For example: data protection law includes provision for disclosure without consent in certain circumstances
- c) There are regulations in place relating to specific organisation, such as the Care Quality Commission (CQC) or Health Protection Agency (part of Public Health England), which support the use of identifiable data for some non-direct healthcare purposes relating to their regulatory function. For example: Under section 63(2)(b) of the Health and Social Care Act 2008, a person authorised to carry out an inspection on behalf of the CQC may access, inspect and take copies of any documents or records held by the Trust, where they consider it 'necessary or expedient' to do so for the exercise of CQC's 'regulatory functions'.
- d) Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001) allows the common law duty of confidentiality to be set aside in specific circumstances where anonymised

information is not sufficient and where patient consent is not practicable. This is managed by the Confidentiality Advisory Group

All organisations that process personal information are required under data protection legislation, to protect it from inappropriate disclosure. Effective pseudonymisation and anonymization techniques enable the Trust to undertake secondary use in a safe, secure and legal way. By removing identifiable data it allows the Trust to share or publish more information with fewer restrictions.

14.0 Data Protection Impact Assessments

All projects and processes that involve personal information or intrusive technologies give rise to potential privacy issues and concerns. To enable the Trust to address the privacy concerns and risks the UK GDPR requires a Data Protection Impact Assessment (DPIA) to be completed, and signed off by the Data Protection Officer. Refer to the Trust Data Protection Impact Assessment Policy and Procedure for more details.

15.0 Confidentiality Audit Approach

With advances in the electronic management of health and employment information, the requirement to monitor access to such confidential information has become increasingly important.

With the move to using more electronic systems, it is imperative that access is strictly monitored and controlled. The movement of confidential information via these methods poses the threat of information falling into the hands of individuals who do not have a legitimate right of access to it.

Failure to ensure that adequate controls to manage and safeguard confidentiality are implemented may result in a breach of that confidentiality, therefore contravening the requirements of Caldicott, the Data Protection Law, the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

The SIRO is responsible for ensuring that audits of security and access arrangements within each area are conducted on a regular basis. Audit should focus on:

- Failed attempts to access confidential information
- Repeated attempts to access confidential information
- Access to confidential by unauthorised persons
- Evidence of shared login sessions/passwords
- Staff awareness of Trust policies and guidelines concerning confidentiality and understanding their responsibilities with regard to confidentiality
- Appropriate use of smartcards
- Appropriate allocation of access rights to systems which contain confidential information
- Appropriate staff access to physical areas
- Storage of and access to filed hard copy patient notes and information
- Security of confidential fax handling
- Confidential information sent or received via email, security applied and email

system used

- Information removed from the workplace – has authorisation been gained either for long term or short term removal?
- Security applied to laptops and portable devices
- Evidence of secure waste disposal
- Use of whiteboards for confidential information
- Information flows of confidential information
- Appropriate transfer and sharing arrangements are in place
- Security and arrangements for recording access applied to manual files both live and archived e.g. storage in locked cabinets/locked rooms

15.1 Confidentiality audits can be carried out in a number of ways:

- Interviews with staff using structured questionnaires
- Notified audit visits with structured questionnaires
- Spot checks at random work areas
- Audit carried out by the Data Owners on electronic records
- Registration Authority (smartcard usage) enhanced reporting facilities
- As part of an investigation into a potential breach of confidentiality/data loss
- Investigation of reports/Caldicott log
- Monitoring of reported incidents

Confidentiality audit results will be collected on a standard template and recorded for analysis and future reporting. Reporting will be to the Data Privacy Committee and will highlight any areas for improvement and learning

If a breach or any risks of breaches of PCD are identified from the audits, matters will be reported and investigated through the Trusts Incident/Serious Incident Reporting Policy and Disciplinary Policy where appropriate.

See Clinical Systems Access and Confidentiality Audit Policy and Procedure for further detail.

16.0 Training Needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory training. The Trust is required to ensure that all permanent staff complete the relevant Data Security Awareness training and maintains a compliance level of 95%.

A record of the event will be recorded on ULearn

The governance group responsible for monitoring the training is the Data Privacy Committee.

17.0 Monitoring Compliance and Effectiveness

| Ref | Minimum Requirements | Evidence for Self-assessment | Process for Monitoring | Responsible Individual / Group | Frequency of monitoring |
|----------|---|------------------------------|---|--------------------------------|-------------------------------|
| 10 21 | Staff adhere to the requirements of the Data Protection Law and understand their obligations in relation to Caldicott and Confidentiality | Section 4.7 Section 7.0 | Confidentiality audits Data Security Awareness Training compliance | Data Privacy Steering Group | As required Bi-monthly |
| 10 | Information Asset Owners undertake annual risk assessments of the assets under their responsibility | Section 4.5 | An annual review of the Information Asset Register | Data Privacy Steering Group | Annually |
| 19 | Privacy Impact Assessments are undertaken where services redesigned/change s in processing/introduction of new technologies | Section 5.5 | DPIA's approved by Data Protection Officer and published | Data Privacy Steering Group | As required |

17.1 Additional Compliance

- General Data Protection Regulation (EU) 2106/679

Compliance with GDPR is mandatory and the Trust will ensure that it keeps an up to date record of all processing activities relating to personal data.

- Data Security and Protection Toolkit

The Trust is required to complete an annual review of Data Privacy compliance by completing the online NHS Digital Data Security and Protection Toolkit

- Reporting of personal data breaches

A personal data breach as defined under Article 4(12) of the Regulation is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Article 33 of the Regulation sets out the obligation on data controllers to report 'without undue delay and, where feasible' not later than 72 hours after having become aware of it, to the supervisory authority – Information Commissioners Office, 'unless the personal data breach is unlikely to result in a risk to the rights

and freedoms of natural persons’

The Trust will report all personal data breaches to the ICO via the NHS Digital online incident reporting tool and in line with the IG SIRI (serious incidents requiring investigation) Checklist

18.0 Standards/Performance Indicators

| TARGET/STANDARDS | KEY PERFORMANCE INDICATOR |
|---|---|
| Data Security and Protection Toolkit – Data Security Awareness Training | 95% of all staff have undertaken Data Security Awareness Training each year |

19.0 References and Bibliography

- The Caldicott Manual
<https://www.ukcgic.uk/caldicott-guardians-manual>
- UK General Data Protection Regulation Guidance - UK Information Commissioners Office website: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- Caldicott Principles – NHS
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942217/Eight_Caldicott_Principles_08.12.20.pdf
- Code of Practice on confidential information
<file:///C:/Users/kirklandsa/Downloads/copconfidentialinformation.pdf>
- Confidentiality: NHS Code of Practice 2003 -
<file:///C:/Users/kirklandsa/Downloads/confidentiality-nhs-cop.pdf>
- Guide to Confidentiality 2013 - [file:///C:/Users/kirklandsa/Downloads/hscic-guide-to-confidentiality_2013%20\(1\).pdf](file:///C:/Users/kirklandsa/Downloads/hscic-guide-to-confidentiality_2013%20(1).pdf)

20.0 Relevant Trust Data Security and Privacy Policies

This is not an exhaustive list and new relevant policies may be developed over time

- Information Security and Risk Policy
- Social Media and Electronic Communications Policy
- Information Governance Forensic Investigation Policy
- Data Privacy Impact Assessment Policy and Procedure
- Individual Information Rights Policy

Training Requirements

Training Needs Analysis

| | |
|--|---|
| Training topic: | Data Security Awareness Training |
| Type of training: (see study leave policy) | <input checked="" type="checkbox"/> Mandatory (must be on mandatory training register) <input type="checkbox"/> Role specific <input type="checkbox"/> Personal development |
| Division(s) to which the training is applicable: | <input checked="" type="checkbox"/> Adult Mental Health & Learning Disability Services <input checked="" type="checkbox"/> Community Health Services <input checked="" type="checkbox"/> Enabling Services <input checked="" type="checkbox"/> Families Young People Children <input checked="" type="checkbox"/> Hosted Services |
| Staff groups who require the training: | All staff groups including Bank, Temporary, Agency, Locum or contractors |
| Regularity of Update requirement: | Annually |
| Who is responsible for delivery of this training? | Learning and Development through ULearn |
| Have resources been identified? | See Learning and Development Prospectus |
| Has a training plan been agreed? | See Learning and Development Prospectus |
| Where will completion of this training be recorded? | <input checked="" type="checkbox"/> ULearn <input type="checkbox"/> Other (please specify) |
| How is this training going to be monitored? | Monthly reports to managers |

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

| | |
|---|--------------------------|
| Shape its services around the needs and preferences of individual patients, their families and their carers | ✓ |
| Respond to different needs of different sectors of the population | <input type="checkbox"/> |
| Work continuously to improve quality services and to minimise errors | ✓ |
| Support and value its staff | <input type="checkbox"/> |
| Work together with others to ensure a seamless service for patients | ✓ |
| Help keep people healthy and work to reduce health inequalities | <input type="checkbox"/> |
| Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance | ✓ |

Stakeholders and Consultation**Key individuals involved in developing the document**

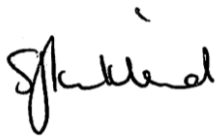
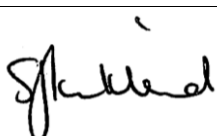
| Name | Designation |
|------------------|----------------------|
| Mary Stait | Data Privacy Manager |
| Hannah Plowright | Data Privacy Officer |
| | |
| | |

Circulated to the following individuals for comment

| Name | Designation |
|-----------------------------------|-----------------------------|
| Members of Data Privacy Committee | |
| Chris Biddle | LHIS Cyber Security Manager |

Due Regard Screening Template

| Section 1 | |
|--|--|
| Name of activity/proposal | Data Protection and Information Sharing Policy |
| Date Screening commenced | 25.08.21 |
| Directorate / Service carrying out the assessment | Finance and Performance/Data Privacy |
| Name and role of person undertaking this Due Regard (Equality Analysis) | Sam Kirkland, Head of Data Privacy/Data Protection Officer |
| Give an overview of the aims, objectives and purpose of the proposal: | |
| AIMS: The policy aims to provide a framework to ensure that the Trust complies with the requirements of the Data Protection Privacy Law (Retained General Data Protection Regulation (EU) 2016/679 - UK GDPR & Data Protection Act 2018), Caldicott Principles and the NHS Code of Confidentiality | |
| OBJECTIVES: Provide staff with key information about how to ensure that they meet their obligations under Data Protection Law, Caldicott and Confidentiality when processing personal and special category data | |
| Section 2 | |
| Protected Characteristic | If the proposal/s have a positive or negative impact please give brief details |
| Age | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Disability | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Gender reassignment | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Marriage & Civil Partnership | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Pregnancy & Maternity | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Race | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Religion and Belief | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Sex | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |
| Sexual Orientation | Positive – the policy is designed to cover the appropriate processing of all personal and special category data managed by the Trust |

| | | | |
|---|--|----------------------------|----------|
| | by the Trust | | |
| Other equality groups? | | | |
| Section 3 | | | |
| Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please <u>tick</u> appropriate box below. | | | |
| Yes | | No | |
| High risk: Complete a full EIA starting click here to proceed to Part B | | Low risk: Go to Section 4. | ✓ |
| Section 4 | | | |
| If this proposal is low risk please give evidence or justification for how you reached this decision: | | | |
| It is a legal requirement to ensure that the handling of management of personal and special category data meets the provisions set out in Data Protection Law and common law duty of confidentiality | | | |
| Signed by reviewer/assessor |  | Date | 03.09.21 |
| <i>Sign off that this proposal is low risk and does not require a full Equality Analysis</i> | | | |
| Head of Service Signed |  | Date | 03.09.21 |

PRIVACY IMPACT ASSESSMENT SCREENING

| | | |
|--|--|-------------------------|
| <p>Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy.</p> <p>The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.</p> | | |
| Name of Document: | Data Protection and Information Sharing Policy | |
| Completed by: | Sam Kirkland | |
| Job title | Head of Data Privacy | Date 25.08.21 |
| Screening Questions | Yes / No | Explanatory Note |
| 1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document. | No | |
| 2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document. | No | |
| 3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document? | No | |
| 4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | No | |
| 5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics. | No | |
| 6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them? | No | |
| 7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private. | No | |
| 8. Will the process require you to contact individuals in ways which they may find intrusive? | No | |
| <p>If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt.dataprivacy@nhs.net</p> <p>In this case, adoption of a procedural document will not take place until review by the Head of Data Privacy.</p> | | |
| Data Privacy approval name: | Sam Kirkland, Head of Data Privacy | |
| Date of approval | 03.09.21 | |

Acknowledgement: Princess Alexandra Hospital NHS Trust

UK GDPR Processing Conditions for Personal Information

Personal data – any data relating to an identifiable person who can be directly or indirectly identified – name; identification number, location data or online identifier

NB personal data that has been pseudonymised can fall within the scope depending on how difficult it is to attribute the pseudonym to an individual

For processing of personal information to be lawful, we must identify a legal basis, sometimes referred to as the “conditions for processing”. It is important to determine, and also document, the legal basis for processing personal data. This becomes more of an issue under the UK GDPR because the legal basis for processing can have an effect on the individual’s rights. Below are the legal bases available for processing personal (and special categories) of information under data protection legislation: Lawfulness of processing **personal data** – Article 6

| Legal conditions for the processing of <u>PERSONAL</u> information | |
|--|---|
| a | Consent of the data subject |
| b | Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract |
| c | Processing is necessary for compliance with a legal obligation |
| d | Processing is necessary to protect the vital interests of the data subject or another natural person |
| e | Processing is necessary for the performance of a task carried in the public interest or in the exercise of official authority vested in the controller |
| f | Necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. <i>(Note that this condition is not available to processing carried out by public authorities in the performance of their tasks)</i> |

Legal obligations

- Health and Social Care (Quality and Safety) Act 2015
- Health and Social Care Act 2012
- Care Act 2014
- The Children Act 1989
- The Children Act 2004

- Childcare Act 2006
- Children (Leaving Care) Act 2000
- Children and Families Act 2014
- National Health Service Act 1977
- National Health Service Act 2006
- Education Act 2002
- Special Education Needs and Disability Regulations 2014
- Localism Act 2011
- Immigration and Asylum Act 1999
- Crime and Disorder Act 1998

See table at the end for the detail of the relevant sections of the above legislation

Sensitive personal data – “special category data”

Racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; processing of genetic data; biometric data (for the purpose of uniquely identifying a natural person); data concerning **health**; data concerning a natural person’s sex life or sexual orientation – shall be prohibited unless one of the following applies:

| Legal conditions for processing SPECIAL CATEGORIES of personal information | |
|--|--|
| a | Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State Law |
| b | Necessary for carrying out obligations under employment and social security and social protection law , or a collective agreement. |
| c | Necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent <i>[The Mental Capacity Act would apply; or if the person is at risk under a Mental Health Act Assessment]</i> |
| d | Processing carried by a not-for-profit body with a political, philosophical, religious or trade-union aim provided the processing relates solely to the members or to former members (or those who have regular contact with it in connection with its purposes) and there is no disclosure to a third party without the consent |
| e | Processing relates to personal data which are manifestly made public by the data subject |
| f | Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |
| g | Necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued |

| | |
|---|---|
| | and which contains appropriate safeguards |
| h | Necessary for the purposes of preventative or occupational medicine , for the assessment of the working capacity of the employee, medical diagnosis , the provision of health or social care or treatment or the management of health or social care systems and services on the basis of union or Member State Law or a contract with a health professional |
| i | Necessary for reasons of public interest in the area of public health , such as protecting against serious cross-border threats to health or ensuring high standards of quality health care and of medicinal products or medical devices |
| j | Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) |

If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of [Schedule 1 of the DPA 2018](#).

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk
19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments

- 27. Anti-doping in sport
- 28. Standards of behaviour in sport

You should identify which of these conditions appears to most closely reflect your purpose.

For some of these conditions, the substantial public interest element is built in. For others, you need to be able to demonstrate that your specific processing is “necessary for reasons of substantial public interest”, on a case-by-case basis.

The public interest covers a wide range of values and principles relating to the public good, or what is in the best interests of society. It needs to be real and of substance. Given the inherent risks of special category data, it is not enough to make a vague or generic public interest argument. You should be able to make specific arguments about the concrete wider benefits of your processing.

For some of the conditions, you also need to justify why you cannot give individuals a choice and get explicit consent for your processing. In most cases, you must have an [‘appropriate policy document’](#) in place.