St Helens and Knowsley Teaching Hospitals NHS Trust

# Code of Confidentiality

**Version No: 6**

**Document Summary:**
This document is a guide to the required practice and responsibility for those who work within or under contract to the Trust concerning confidentiality of staff and patient information.

| | | |
|---|---|---|
| **Document status** | Approved | |
| **Document type** | Policy | **Trust wide** |
| **Document number** | STHK0117 | |
| **Approving body** | Information Governance Steering Group | |
| **Date approved** | 16/11/2021 | |
| **Date implemented** | 16/11/2021 | |
| **Review date** | **30/11/2024** | |
| **Accountable Director** | Director of Informatics | |
| **Policy Author** | Head of Risk Assurance and Data Protection Officer | |
| **Target audience** | All staff | |

**The intranet version of this document is the only version that is maintained. Any printed copies should therefore be viewed as "uncontrolled", as they may not contain the latest updates and amendments.**

# Document Control

| Section 1 – Document Information | |
|---|---|
| **Title** | Code of Confidentiality Policy |
| **Directorate** | Informatics |
| **Brief Description of amendments** | |
| See Section 3 'Brief Summary of Changes' | |
| **Does the document follow the Trust agreed format?** | Yes |
| **Are all mandatory headings complete?** | Yes |
| **Does the document outline clearly the monitoring compliance and performance management?** | Yes |
| **Equality Analysis completed?** | Yes |

| Section 2 – Consultation Information*<br>*Please remember to consult with all services provided by the Trust, including Community & Primary Care | | | |
|---|---|---|---|
| **Consultation Completed** | ☐ Trust wide ☐ Local ☑ Specific staff group | | |
| **Consultation start date** | Click here to enter a date. | **Consultation end date** | Click here to enter a date. |

## Section 3 – Version Control

| Version | Date Approved | Brief Summary of Changes |
|---|---|---|
| 6 | 16/11/2021 | • Main changes: reordered sections to enable the reader to follow and find relevant sections easier; removal of consent where is stated consent was necessary to process data for direct care and updated to reflect the UK GDPR lawful basis.<br>• Section updated to reflect the scope of the policy and information removed to the Introduction section – **Section 1 (Scope)**<br>• Additional information taken from the previous Scope added to Introduction section and clearer explanation of what Information Governance is – **Section 2 (Introduction)**<br>• Paragraph moved from Introduction to Statement of Intent, first paragraph – **Section 3 (Statement of Intent)**<br>• Definitions section fully updated and added to – **Section 4 (Definitions)**<br>• Change to duties and responsibilities. Further detail provided for the following: DPO, IAO, IAM/IAA IG Team, IGSG, IT Tech / IT Security team, Staff and workers - **Section 5 (Duties, Accountabilities and Responsibilities)**<br>• Section 6 renamed from Confidentiality Code of Conduct Policy Processes to Confidentiality Code of Conduct Policy Principles and areas classed as 'processes' moved to a new section (7), the principles left under this section – **Section 6**<br>• Openness section updated and expanded – **Section 6.1**<br>• New section added on Legal Compliance (Legislation) – **Section 6.2** |

| | | |
|---|---|---|
| | | • New section added on UK GDPR / Data Protection Principles – **Section 6.2.1**<br>• New section added on Consent and Other Lawful Basis for Processing Personal Data – **Section 6.2.2**<br>• Information Security expanded– **Section 6.3**<br>• New section name added and processes sitting under this section re-ordered – **Section 7 (Confidentiality Code of Conduct Policy Processes)**<br>• New section added under Record Keeping section 7.2 – Section 7.2.1 **(Collecting only what is necessary)**<br>• New section added under Record Keeping section 7.2 – **Section 7.2.2 (Recording the data accurately)**<br>• More detail added to Telephone Enquiries – **Section 7.3 (Verbal Communications and Telephone Enquiries)**<br>• Information Sharing section expanded to include 7 golden rules of information sharing – **Section 7.4 (Information Sharing)**<br>• New section added under Information Sharing, when to share for direct patient care – **Section 7.4.1. (Sharing for direct care purposes)**<br>• New section added under Information Sharing, when to share for non-direct patient care - **Section 7.4.2. (Sharing for non-direct care purposes)**<br>• Faxing banned in NHS April 2020, this section updated to reflect the change – **Section 7.5.2 (Faxing)**<br>• Removal of reference to NHS.net to achieve Email Secure Standards Accreditation – **Section 7.5.3 (Email)**<br>• Password Protection section expanded – **Section 7.9.1**<br>• Home working section expanded to include advice on printing **– Section 7.15**<br>• New Appendix page added – Appendix D **(Caldicott Principles)**<br>• New Appendix page added – Appendix E **(UK GDPR Lawful Basis)** |

| **Section 4 – Approval** – *To be completed by Document Control* | | | |
|---|---|---|---|
| **Document Approved** | ☑ Approved ☐ Approved with minor amendments | | |
| **Assurance provided by Author & Chair** | ☑ Minutes of Meeting ☐ Email with Chairs approval | | |
| **Date approved** | 16/11/2021 | **Review date** | 30/11/2021 |

| **Section 5 – Withdrawal** – *To be completed by Document Control* | |
|---|---|
| **Reason for withdrawal** | ☐ No longer required ☐ Superseded |
| **Assurance provided by Author & Chair** | ☐ Minutes of Meeting ☐ Email with Chairs approval |
| **Date Withdrawn:** | Click here to enter a date. |

# Contents

## 1. Scope

This policy is applicable to all staff who are directly employed by and for whom St Helens and Knowsley Teaching Hospitals NHS Trust (hereafter referred to as the Trust) has a legal responsibility for, who will need access to personal, confidential and / or corporate information at the Trust. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the Trust. The collective term 'staff' is used throughout this policy to mean all these groups.

## 2. Introduction

All NHS employees are bound by a Common Law Duty of Confidentiality to protect personal identifiable information, known as personal data that they process during the course of their work. This is not just a requirement of their contractual responsibilities, but also a requirement of the data protection legislation known as the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA 2000). It is also required to meet Information Governance (IG) / Information Security / NHS specifications and requirements mainly relating to the National Data Guardian's Data Security Standards and other related legislation, guidance and contractual responsibilities to support the assurance standards of the Data Security and Protection Toolkit (DSPT), which the Trust completes annually. In addition, Health Professionals have standards laid down in their own Professional Codes of Conduct. It is essential therefore, that staff understand what they need to do to keep information, specifically personal and confidential data, safe and secure.

Information Governance is the way in which the NHS handles all organisational information. It pulls together all the information handling requirements into one framework – in particular the personal and confidential information of patients / service users / clients and staff. It allows organisations and individuals to ensure that personal data is dealt with legally, securely, efficiently and effectively, in order to protect confidentiality and assists in the delivery of the best possible services and care.

All staff are required to keep personal data relating to patients or staff strictly confidential. Personal data is not only found in a patient's health record it may be recorded in personnel records, databases, waiting lists, referral letters, discharge summaries, invoices etc.

The Trust has four main aims with regard to Confidentiality these are to:

- Protect – keep personal data secure from unauthorised access
- Inform – ensure that all patients and staff are aware of how their information is used
- Choice – allow patients and staff to decide whether their information can be disclosed or used in particular ways, subject to legislation
- Improve – always look for better ways to protect, inform, and provide choice to the individual

The Trust is committed to adhering to data protection legislation and national standards. This means ensuring that all personal data is processed fairly, lawfully, securely, efficiently and transparently as far as possible so that the public can:

- Understand the reasons for processing personal data
- Gain trust in the way the Trust processes data
- understand their rights regarding the processing of their personal data

This policy is to facilitate effective working across the Trust and to provide all staff with guidance on what to do when they are processing personal data.

The Trust recognises the importance of reliable information, both in terms of clinical management of individual service users and the efficient management of services and resources. Information Governance plays a key part in supporting Clinical Governance, Service Planning and Performance Management.

## 3. Statement of Intent

The purpose of this policy is to re-enforce the Trust's commitment to Information Governance.

This Policy sets out the principles by which the confidentiality, integrity and availability of personal data and corporate information will be managed within the Trust whether this information is stationary or in transit. This policy provides staff with clear guidance on how to manage the different forms of information and clarifies their roles and responsibilities.

The principle behind this Code of Practice is that no member of staff shall knowingly breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's systems or controls in order to do so.

Staff should consider all information to be sensitive and apply the same standards to all information they come into contact with.

The awareness and behaviour of staff is the most important element in any organisation's information security, therefore, staff should:

- Make sure that any personal data about patients / service users / clients and staff that they hold or control (process), is effectively protected at all times against improper disclosure/loss. Many disclosures/losses are unintentional and avoidable
- Ensure that errors give rise to learning – lessons can usually be learnt from errors allowing good practice for the future
- If there is an error; record the incident on Datix, the Trust incident and risk management system. If in any doubt contact the Information Governance Team
- Share any good practice - if staff identify ways in which information handling can be improved in their work area this should be shared with colleagues
- Encourage others to share their good practice
- Promote teamwork as a key part of ensuring that all personal data is treated with respect and with regard for confidentiality
- Make sure they are aware of their responsibilities whilst using social networking sites, e-mail, and the internet

**Basic Principles**

To enable the Trust and its staff to:

- Hold information securely and confidentially
- Obtain information fairly and efficiently
- Record information accurately and reliably
- Use information effectively and ethically
- Share information appropriately and lawfully

Any personal data given for one purpose must not be used for another purpose without a lawful basis being identified as it may breach confidentiality (consult with the IG team). Staff must remember:

- An individual's right to confidentiality is protected by law

- Individuals have the right to know what information is being collected and why, and the reasons for sharing that information
- In some circumstances an individual has the right to choose how their personal data is to be used or who is allowed to see it
- Every member of staff has an obligation to:
    - Protect confidentiality
    - Ensure that any person asking for another's information is authorised to have access to it
    - Understand their responsibility in relation to confidentiality
    - Understand and follow the Trust's policies relating to confidentiality

This policy covers all aspects of information within the Trust including (but not limited to):

- Service User information
- Personnel Information
- Organisational Information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems – paper and electronic
- Transmission of information – e-mail, post, telephone and fax

This policy covers all information systems purchased, developed and managed by or on behalf of the Trust and its partners, including any individual directly employed or otherwise by the Trust. It is important that staff understand that disclosure and sharing of personal data is governed by the requirements of certain Acts of Parliament, and Government and NHS guidelines. These include:

- UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- Common Law duty of Confidentiality
- The Children's Act 1989 & 2004
- Health & Social Care Act 2012
- Records Management Code of Practice (2021)
- The Human Rights Act 1998
- Caldicott Report & Principles
- The Freedom of Information Act 2000
- Access to Health Records Act 1990
- Crimes and Disorder Act 1998
- Public Interest Disclosure Act 1998
- Information Security NHS Code of Practice Police and Justice Act 2006

This Policy has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal (Disciplinary Policy and Procedure).

## 4. Definitions

| Definition | Meaning |
|---|---|
| **Personal Data** | Also referred to as personal identifiable information. It is anything that contains the means to identify an individual and may consist of: |

| | |
|---|---|
| | • a person's name, address, full post code, date of birth;<br>• pictures, photographs, videos, audio tapes or other images of patients;<br>• NHS number and local patient identifiable codes;<br>• 'Online identifiers' include IP addresses and cookie identifiers which may be personal data;<br>• anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified. |
| **Sensitive Personal Data / Special Category Data** | Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated within legislation. Under the Data Protection Act 2018, this type of data is now known as 'Special Category' data and relates to data about an individual's race; ethnic origin; politics; religion; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. |
| **Confidential Information** | Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.<br><br>Information may be held in paper or electronic format, computer file or printouts, video, photograph or even heard by word of mouth.<br>It includes information stored on portable devices such as laptops; mobile phones; removable media; recording devices and digital cameras etc.<br>It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any company e.g. Trust business confidential information. |
| **Anonymised Data** | This is information which does not identify an individual directly, and information which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that might support identification. |
| **Pseudonymised Data** | Similar to anonymised data in that in the possession of the information holder / recipient it cannot be used by the holder to easily identify an individual. However, it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not. |
| **Processing** | Processing means any operation or set of operations which are performed on personal data or on 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. |
| **Consent** | Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. |
| **Data Controller** | This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this case The Trust. |
| **ICO** | Information Commissioner's Office - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy. |

# 5. Duties, Accountabilities and Responsibilities

## 5.1. Chief Executive

As the Head of the Organisation, the Chief Executive has overall responsibility for the strategic and operational management of the Trust including and ensuring that Trust policies comply with all legal, statutory and good practice guidance requirements.

## 5.2. Senior Information Risk Owner (SIRO)

The Director of Informatics is the Trust's SIRO and takes overall ownership of the Organisation's Information Risk Policy, and acts as the champion for information risk on the Board and provides written advice to the Chief Executive on the content of the Annual Governance Statement (AGS) in regard to information risk.

The SIRO is expected to understand the strategic business goals of the Organisation and how other NHS Organisations' business goals may be impacted by information risks, and how those risks may be managed.

The SIRO will implement and lead the NHS Information Governance (IG) risk assessment and management processes within the Organisation and advise the Board on the effectiveness of information risk management across the Organisation.

## 5.3. Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that the Trust processes satisfy the highest practical standards for handling patient information and provide advice and support to Trust staff as required.

The role of the Guardian is to safeguard and govern uses made of patient information within the Trust, as well as data flows to other NHS and non-NHS organisations. Caldicott Guardianship is a key component of broader information governance.

The Guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable patient information and, where appropriate, the transfer of that information to other bodies.

The Guardian utilises the UK Caldicott Guardian Council's 'A Manual for Caldicott Guardians' to assist them in embedding the Caldicott principles within the Trust (refer to Appendix D for the full list of the Caldicott principles). This document sets the role of the Caldicott Guardian within an organisational Caldicott/Confidentiality function which is itself a part of the broader Information Governance agenda.

Both the Caldicott Guardian and the SIRO will be assisted in their work by a comprehensive support structure.

The Trust also has a named Deputy Caldicott Guardian who is available to act as deputy for the Caldicott Guardian when they are not available.

## 5.4. Data Protection Officer

The UK GDPR requires that all public authorities nominate a Data Protection Officer (DPO). Section 7 of the Data Protection Act 2018 defines the Trust as a public authority and as such it must nominate a DPO.

The DPO role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance.

Article 39 of the UK GDPR defines the duties of the DPO as:

- Informing and advising employees about their obligations to comply with the UK GDPR, the Data Protection Act and other legislation and monitoring compliance with such legislation
- Monitoring compliance with data protection policies and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of an IG Framework document supported by relevant policies and procedures
- Raising awareness of data protection issues with staff and at a senior level
- Raising awareness of data security training and monitoring compliance
- Providing advice and guidance on Data Protection Impact Assessments (DPIAs) as per Article 38 of the UK GDPR
- To be the first point of contact with the supervisory authorities, including the ICO, and individuals whose data is being processed
- Developing and maintaining comprehensive and appropriate documentation
- Monitoring compliance and carrying out audits
- Maintaining expert knowledge in data protection

The DPO for the Trust is the Head of Risk Assurance.

## 5.5. Information Asset Owner

The SIRO is supported by Information Asset Owners (IAOs). Their role is to understand what information/personal data is held, how it is managed and who has access, and why, to information systems in their own area. As a result they are able to understand and address risks to the information assets they own and to provide assurance to the SIRO on the security and use of those assets. UK GDPR requires that records of information processing are undertaken, therefore, it is essential that IAOs review / maintain and update their Information Asset Registers and Data Flow Mapping Registers as and when required for their area. The IG Team support the IAOs in fulfilling their role.

The Executive Leads will be the Information Asset Owners who may delegate this role to the Information Asset Manager and Administrator.

In addition they will:

- Lead and foster a culture that values, protects and uses information for the success of the Trust and benefit of its patients and staff
- Know what information comprises or is associated with the asset(s), and understand the nature and justification of information flows to and from the asset
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy

- Understand and address risks to the asset and provide assurance to the SIRO
- Ensure there is a legal basis for processing and for any disclosures
- Ensure all information assets are recorded on the Information Asset Register (IAR) and maintained
- Refer queries about any of the above to the Data Protection Officer and Information Governance team, and
- Undertake specialist information asset training as required

### 5.6. Information Asset Managers / Administrators

An IAO may delegate responsibility for management of confidential information to an Information Asset Manager (IAM) or Information Asset Administrator (IAA). While the IAM and IAA may be responsible for the proper handling of information, the IAO remains accountable**,** therefore the IG Team will need to ensure that the IAM and IAA understands, and has the required competencies to undertake these responsibilities.

Delegated responsibilities typically include:

- Managing the joiners, movers and leavers process within the team
- Ensuring all team members keep their training up-to-date
- Granting and revoking access to confidential information
- Recognising potential or actual security incidents
- Consulting the IAO on incident management
- Ensuring that risk assessments and other documents are accurate and maintained

The IAM maybe a department / senior manager and an IAA maybe the team members.

### 5.7. Directorate / Operational Directors and Senior Manager

The Directorate / Operational Directors are responsible for ensuring that all directorate staff are aware and implement Information Governance policies including this policy, procedures and standards. They should ensure that the policy and its supporting standards and guidelines are built into local processes. They are also responsible for ensuring staff are updated in regard to any changes in this policy.

### 5.8. The Information Governance Team

The Information Governance (IG) Team is responsible for advising on strategic direction, the development of policy and guidance for the Trust, and also operational support to the Trust on Information Governance compliance.

Key tasks include:

- Developing and maintaining comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of a data security (IG) framework document supported by relevant policies, procedures and guidance
- Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements within the Trust
- Establishing working groups, if necessary, to co-ordinate the activities of staff with IG responsibilities
- Ensuring assessments and audits of IG are implemented and reported
- Ensuring that annual assessments and regular improvement plans / progress reports are prepared
- Ensuring that the approach to information handling is communicated to all staff and made available to the public
- Monitoring the Trust's IG training compliance

- Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards
- Monitoring information handling activities to ensure compliance with the law and relevant guidance
- Providing a focal point for the resolution and / or discussion of data security / information governance issues

### 5.9. Information Governance Steering Group

The Information Governance Steering Group is a standing committee accountable to the Trust Board via the Risk Management Council. The Group consists of various key members of the Trust including the Caldicott Guardian, SIRO, Data Protection Officer, IG Manager, Head of IT Security Lead and will:

- Oversee the implementation of the Information Governance strategy, policy and completion of the annual baseline assessment, Data Security and Protection Toolkit and associated work programme and ad hoc Information Governance related work stream projects
- Provide the members with updates on key data security initiatives such as Data Protection Impact Assessments (DPIAs), FOI compliance, lesson learned from incidents, IG training / monitoring and confidentiality audit reviews etc.
- Provide the Trust Board with the assurance that effective Information Governance best practice mechanisms are in place within the Organisation

### 5.10. IT Technical / IT Security Staff

IT technical and security staff ensure that the technology we use is safe and secure. They provide advice, guidance and support regarding any IT technical issues. The IT provider currently ensures that cyber security standards are in place to prevent / detect and deter cyber-attacks as much as possible.

### 5.11. Staff and workers

All staff are responsible for ensuring they are aware of the Information Governance requirements including confidentiality and ensuring they comply with these on a day to day basis.

Staff will receive instruction and direction regarding the policy from several sources:

- DPO
- Information Governance team
- Policy / strategy and procedure manuals
- Line manager
- Specific training course
- Other communication methods, for example, team meetings; and
- Trust website

All staff are mandated to undertake mandatory information governance training in line with the training needs analysis programme as agreed by the IG Steering Group (section 8).

The importance of Information Governance will be addressed with all relevant staff as part of their induction into their individual department.

All staff must make sure that they use the organisation's IT systems appropriately and adhere to this Policy.

A full list of staff responsibilities around e-mail and internet use is shown in Appendix A.

## 6. Confidentiality Code of Conduct Policy Principles

There are four key inter-linked strands to the Confidentiality Code of Conduct Policy which you need to be aware of:

- Openness
- Legal Compliance
- Information Security
- Information Quality Assurance

### 6.1. Openness

- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information
- The Trust has an obligation as a Data Controller to notify the ICO of the purposes for why it needs to process personal data. Notification monitoring within the organisation is carried out by the IG team. Individuals can obtain full details of the organisation's data protection registration / notification from the ICO website: (www.ico.gov.uk)
- Non-confidential information about the Trust and its services will be available to the public through a variety of media, in compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004. The organisation's Publication Scheme will continue to meet the requirements of the ICO's Model Scheme for health bodies, where information is made available, usually on the Trust's website
- The Trust will ensure that the principles of Caldicott and the regulations outlined in the current Data Protection Legislation (UK GDPR and DPA 2018) underpin the management of personal data at all times
- The Trust needs to share personal information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest. The Trust will ensure that when sharing it does so in accordance with the current Data Protection legislation
- All service users, patients and staff should have ready access to information relating to themselves. Knowing their data rights as a patient and / or a member of staff. There are clear procedures and arrangements for handling requests for personal information from individuals detailed in the organisation's Subject Access Request / Access to Health Records Policy
- The Trust will undertake or commission regular assessments and audits of its policies and arrangements for openness
- The Trust will publish a Privacy Notice consistent with the requirements of the Data Protection Act 2018, to provide individuals with information around the purposes for processing their personal data

### 6.2. Legal Compliance (Legislation)

- Information Governance encompasses legal requirements (Acts of Parliament), ethical considerations, national guidance and best practice in information handling which the Trust need to abide by (see section 3 for the list). Monitoring is conducted by the Information Governance Team
- The Trust processes personal data about its staff, patients and other individuals for various purposes (for example, the effective provision of healthcare services). To comply with the current Data Protection legislation information must be 'processed,' collected and used fairly, stored safely and not disclosed to any unauthorised person. The current Data Protection legislation applies to both manual and electronically held data for living persons. The lawful and correct treatment of personal data is key to maintaining confidence within the Trust and the individuals with whom it deals. The Trust will comply

with the Data Protection Principles setting out the main responsibilities for organisations (see section 6.2.1)

- Patient and/or staff information will be shared with other agencies in accordance with agreed protocols and relevant legislation (e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998, Protection of Children Act 1999, Terrorism Act 2000) and the appropriate lawful basis for sharing will be identified
- Where appropriate informed and explicit consent will be sought from the individual and recorded, for the collection, processing and disclosure of data if this is deemed as the appropriate lawful basis
- Individuals will be informed of the purpose for which information is being collected / processed and who may access it. This will be via the Trust's Privacy Notice (Article 5 (a))
- The Trust will comply with the provisions of Article 12 - 22 of the UK GDPR and will establish and maintain appropriate and adequate administration arrangements for responding to individual right requests (e.g. Subject access) within the timescales defined under the Act
- The Trust will undertake or commission an external assessment of its Information Governance Policies in line with the Data Security and Protection Toolkit annual review in order to check its compliance with legal requirements
- The Trust will establish and maintain policies to ensure compliance with the common law duty of confidentiality and all relevant Acts of Parliament

### 6.2.1.UK GDPR/ Data Protection Principles

The current Data Protection legislation and the common law duty of confidentiality should underpin the development of any information sharing decision. As Data Controllers, the Trust has a duty to comply with the Data Protection Principles (Article 5 of the UK GDPR):

**Lawful, fair and transparent processing** – this principle emphasises transparency for all individuals. When personal data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the individual

**Purpose limitation** – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Simply put, this principle says that organisations should not collect any piece of data that doesn't have a specific purpose

**Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant and limited. Organisations should only collect and compile data for the purpose they have identified and the minimum amount necessary, storing the minimum amount of data required for their purpose

**Accurate and up-to-date processing** – this principle requires organisations to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing

**Limitation of storage in the form that permits identification** – this principle discourages unnecessary data and replication. It limits how the data is stored and

moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached

For example, organisations should prevent users from saving a copy of a patient/staff list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is goes against legislation

**Integrity, Confidential and Secure** – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting, and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects

The UK GDPR also introduces the principle of accountability:

**Accountability and liability** – this principle ensures that organisations can demonstrate compliance with the law. Organisations must be able to demonstrate to the governing bodies that they have taken the necessary steps to protect individual's personal data

### 6.2.2. Consent and Other Lawful Basis for processing personal data

Consent to processing personal data must not be confused with consent to treatment. The two are separate and for the purposes of this policy and IG the focus is on processing personal data.

Under the UK GDPR there are 6 lawful bases and one must be appropriately selected when the Trust processes personal data. The Trust cannot legally process personal data without a lawful basis. Pre the UK GDPR, the most common and relied upon legal basis for the majority of processing of personal data was consent. Consent is still included in the UK GDPR but not relied upon for healthcare purposes and many other areas of processing. Please refer to Appendix E for the UK GDPR lawful bases.

Where the Trust is processing data for the purposes of 'Direct Patient Care' consent is not required and another legal basis called 'Public tasks' should be applied. This means that explicit consent is not required, although there is still a need to notify patients how their data is being used – this is normally detailed in a Privacy Notice, even posters and leaflets.

The ICO recognise that for 'Direct Patient Care' consent is not appropriate, as to apply consent properly the patient has the right to withdraw their consent at any time, this could be during treatment, when there is a need to view the patient's record for example – creating a patient and clinical risk.

Consent however maybe considered for other uses of personal data for example, research and training. The IG team will be able to advise on the appropriate legal basis after assessing the purpose. If consent is sought there is a need to be clear for what purpose/s, gaining consent is not seen as a 'gateway' to processing / sharing personal data for absolutely anything. For example, in medical photography they may gain consent for processing the personal data for

training purposes, this does not mean that this data can be shared for research as well unless they have been clear it is for this purpose too.

The IG team are responsible for advising on the appropriate legal basis for processing personal data, for example, if consent they will ensure the appropriate steps are followed to make sure the consent model complies with the law and will offer advice and what needs to be done.

### 6.3. Information Security

- The Trust will establish, implement and maintain policies for the effective and secure management of its information assets and resources
- The Trust will promote effective confidentiality and security practice to its staff through its Information Governance policies, procedures and training. These policies and procedures are available on the Trust Intranet and from the IG Team
- Systems will be established to ensure that corporate records including health records are available and accessible at all times
- Effective authorisation procedures for the use and access to personal confidential information and records, ensuring that there are strong access controls for all information systems in use at the Trust
- The Trust will ensure there are audit trails and monitoring of user activity built-in to information systems
- The Trust will ensure that all portable electronic media is encrypted
- The Trust will maintain an accurate and up-to-date Information Asset Register
- The Trust will ensure the secure disposal of data and hardware when disposal is required
- The Trust will undertake or commission regular assessments and audits of its information and IT security arrangements as part of the Data Security and Protection Toolkit annual review
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training. These policies and procedures are available on the Trust Intranet and from the IG Team
- The Trust will undertake Data Protection Impact Assessments, Supplier's Due Diligence to determine appropriate security controls are in place for existing or potential information systems
- The Trust will establish and maintain incident reporting procedures which will include the monitoring and investigation where appropriate, of reported instances of actual or potential breaches of confidentiality or information security

### 6.4. Information Quality Assurance

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The Trust will promote records management through policies, procedures and training
- The Trust will undertake or commission regular assessments and audits of its information quality and records management arrangements
- Information Asset Owners and Line Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards
- Quality control in record conversion is extremely important to the Trust. Where information is scanned there is the potential for loss of some of the information. In all cases, the organisation will review the information loss and make a decision as to whether the loss is acceptable

- The Trust will refer to the current Records Management Code of Practice as its standard for records management
- Please also see the Trust Corporate Records Policies and Health Records Policies available on the Trust Intranet site

# 7. Confidentiality Code of Conduct Policy Processes

## 7.1. Informing Individuals

It is a requirement under the UK GDPR to be transparent and open about how the Trust processes personal data to all the individuals they serve.

### 7.1.1 Informing Patients effectively

Consider if patients would be surprised to learn that their information was being used in a particular way. If so then they are not being effectively informed.

To inform patients correctly staff should:

- Check, where practicable, that information leaflets on patient confidentiality and information disclosure have been given to the patient, read and understood
- Make clear to patients when information is recorded or health records are accessed
- Make clear to patients who they are or who they will be disclosing information to
- Check patients are aware of their choices, have no concerns, queries or objections concerning how their information is disclosed and used
- Answer any queries personally or direct the patient to others who can answer their questions
- Respect the rights of patients including their right to have access to their health records through Trust Subject Access /Access to Health Records procedures
- Refer patients to the Trust's Privacy Notice for the public which is available on the website should they require further information about how their personal data is used. Should patients require further detail, staff should refer them to the Trust Information Governance team at IG@sthk.nhs.uk

### 7.1.2. Providing Patients with Choice

Patients have different needs and values – this must be reflected in the way they are treated both in terms of their medical condition and the handling of their personal information. Patients have the right to discuss whether or not to accept a form of care and the information disclosure needed to provide that care, and to discuss whether or not information that can identify them can be used for non-healthcare purposes.

Under the UK GDPR for direct care purposes consent is not required and another legal basis called 'public tasks' is applied. This means that explicit consent is not required in these circumstances, however patients must still be informed about how their personal data will be used and should they have any concerns regarding the use of their personal data they should discuss this with a health care professional. Where the health care professional believes that processing the personal data is in the best interests of the patient the processing will continue.

**Staff must:**

- Inform patients before using their personal data in ways that do not directly contribute to or support the delivery of their care and check with the IG team as to whether consent is required

- Respect patients decisions to restrict the disclosure or use of information except where exceptional circumstances apply – this can be overridden if it is deemed that processing personal data is in the patient's best interest, i.e. without would cause a clinical / patient safety risk
- Communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to, or restrict the disclosure of information. Record that decision in the patient's notes

#### 7.1.3. Informing Staff effectively

As detailed in section 7.1.1, similar to patients, all staff need to be aware of how their personal data is processed. The Trust has a Staff Privacy Notice available on the Intranet should staff require further information on how their personal data is used.

### 7.2. Record Keeping

#### 7.2.1. Collecting only what is necessary

You should only collect as much personal data as is necessary for the agreed purpose, and no more. The information collected must be adequate but not excessive. Most healthcare records for example are by necessity very detailed, but they must nevertheless be accurate and relevant. Where information is extracted for other agreed purposes (for example audit) there should be a sound rationale for every piece of information that is used and a legal basis which your IG Team will be able to advise on. Where personal data is being processed for purposes for other than direct care or for contact requirement, personal identifiers should be removed from the data if they are not strictly necessary for the intended use.

#### 7.2.2. Recording the data accurately

You have a legal obligation to ensure that any personal data you are processing is accurate. Personal data is regarded as inaccurate if it is incorrect or misleading as to any matter of fact. Individuals (patients and staff) have a legal right to have factual inaccuracies corrected or removed from records, and to have an entry made in their record if they disagree with a statement of opinion.

#### 7.2.3. Paper-based data / Manual records

You should adhere to the following process when processing any paper records, which must be:

- Formally booked out from their normal filing system if there is a requirement to, check with line manager
- Tracked if transferred, using the Trust record tracking procedures
- Returned to the filing location as soon as possible after use
- Stored securely whilst temporarily required within any clinic or office, so that the record can be located if needed urgently
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons
- Held securely within the Department

Staff must not use public transport, which includes the hospital shuttle bus to transport patient or staff information; please contact the Health Records department who will provide a driver.

#### 7.2.4. Electronic records

You should adhere to the following principles when accessing any electronic records:

- Never look, copy, download or make any unauthorised use of any clinical or personnel information relating to your family, friends, patients or people in the public eye, who are treated by the Trust. Access to clinical, information is only acceptable if you are directly involved in the clinical care of a patient
- Always log out of any computer system or application when you leave your desk or no longer need access
- Not leave a terminal unattended and logged in
- Not share logins with other people. If other employees have need to access, then this will be organised for them upon application to the Informatics Department – not by using somebody else's user name or password
- Not reveal passwords or share smart cards with other members of staff
- Change passwords at regular intervals when prompted, or if your password might have been compromised
- Avoid using short passwords, or using names or words that are known to be associated with them (e.g. children or pet names or birthdays). Further information on passwords management is available from the Informatics Department
- Where possible it is best to protect the monitor view to avoid patient's information being seen
- Not save any work that contains personal data to a shared drive where it would be accessible to unauthorised users (i.e. staff member from another team)

### 7.2.5. Patient Records

Maintaining proper records is vital to patient care. If records are inaccurate, decisions that could potentially cause harm to the patient may be made. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that could lead to better treatments in the future. The practical value of privacy enhancing measures and anonymised techniques will be undermined if the information they are designed to safeguard is unreliable.

Patient's records should be factual, consistent and accurate and;

- Be written down as soon as possible after the event has occurred providing current information on the care and condition of the patient
- Be written clearly, legibly and in such a manner that they cannot be erased
- Be written in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly
- Be accurately dated, timed and signed or otherwise identified with the name of the author being printed alongside the first entry
- Be legible on any photocopies
- Be written wherever applicable with the involvement of the patient or carer
- Be clear, unambiguous (preferably concise) and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions
- Be consecutive
- Use standard techniques and protocols (for electronic records)
- Be written so as to be compliant with the Race Relations Act and the Disability Discrimination Act

Be relevant and useful:

- Identify problems that have arisen and the action taken to rectify them
- Provide evidence of the care planned, the decision made, the care delivered and the information shared
- Provide evidence of actions agreed with the patient (including consent to treatment and/or consent to disclose information)

And include:

- Medical observations; examinations, tests, diagnosis, prognoses, prescriptions and other treatments
- Relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment
- Facts presented to the patient
- Correspondence from the patient or other parties

Patient records should not include:

- Unnecessary abbreviations or jargon
- Meaningless phrases, irrelevant speculation or offensive subjective statements
- Irrelevant personal opinions regarding the patient (See Management of Health Records Policy available on the Intranet)

### 7.2.6. Staff Records

The same principles as listed in section 7.2.5 must be applied when processing staff data. In addition staff should:

- Never view their own, friends, family, colleagues or high profile patient's medical records. To do so would be a breach of this policy and could result in dismissal from employment. Access to clinical information is only acceptable if you are directly involved in the clinical care of a patient. An exception to this is if they have completed the necessary documentation via Access to Records, Legal Services Department and have the necessary permission to do so
- Never disclose to a third party or use the data for a purpose other than the original intent without employees being informed, and consent given or where there is a statutory, legal requirement to disclose
- Keep the personal data up to date and accurate
- Keep the record in accordance with the Human Resources Department procedures
- Be aware that any Subject Access requests to personnel records will follow both the HR Department written procedures as well as the Trusts Subject Access Request / Access to Health Records Policy

## 7.3. Verbal Communication and Telephone Enquiries

- A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality, particularly in modern open plan offices. Care should be taken to ensure that confidentiality is maintained in such discussions
- Where information is transferred by phone, or face-to-face, care should be taken to ensure that personal details are not overheard by other staff who do not have a "need to know". Where possible, such discussions should take place in private locations and not in public areas, common staff areas, lifts, etc.
- Messages containing personal information should not be left on answer machines.
- Where information is requested by telephone:
    - Always try to check the identity of the caller and check whether they are entitled to the information they request. This may require you asking the patient if they want their information shared with callers. In most cases patients will be happy for limited information to be shared but we need to be sure
    - If a call is requesting confirmation that a patient is on a ward do not just provide that information without the consent of the patient
    - Consider setting up a code word for patients which they will share with those with whom they wish information to be shared, this will ensure we respect their wishes and protect their confidentiality

- Take a number, verify it independently and call back if necessary

### 7.4. Information Sharing

Who can you share information with, and what information can you share? Staff often get confused as regards what they can and cannot share. Remember that UK GDPR and IG are not barriers to appropriate sharing. This has been clarified by the new Caldicott principle which was introduced in 2013 and states that:

'**The duty to share information can be as important as the duty to protect patient confidentiality'.**

This is the guiding principle when considering the sharing of patient information. Refer to Appendix D for full list of the Caldicott Principles.

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The Trust must ensure that mechanisms are in place to enable reliable and secure exchange of data within legal limits.

Seven golden rules of Information Sharing are:

1. Remember that the UK GDPR, DPA 2018 and Human Rights Act 1998 are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately
2. Be open and honest with the individual from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so
3. Seek advice from other practitioners, the IG Team / DPO if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible
4. Under the UK GDPR and DPA 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so (i.e. direct patient care), such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared
5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion and is shared securely
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

#### 7.4.1. Sharing for direct care purposes

Staff sharing personal data with other organisations for direct care purposes will not need to rely on consent as a lawful basis for processing and do not necessarily need an Information Sharing Agreement in place. It may be good practice to have one and to also log this information on an Information Asset Register.

#### 7.4.2. Sharing for non-direct care purposes

There will be times when personal data needs to be shared for purposes other than direct care, for example staff information may be shared for payroll purposes if another organisation is processing the data on behalf of the Trust, or where patient data maybe required for training purposes. In these circumstances Information Sharing Agreements are required to be put in place when information is being shared for a non-direct care purpose and this must specifically state the lawful basis or overriding interest for sharing.

For further advice and guidance regarding information sharing and if in doubt about whether personal data can be shared please contact the IG Team.

### 7.4.3. Capacity to Share Information

You owe a duty of confidentiality to all patients, past or present, even if they are adults who lack capacity and where it is **not for direct care**. You may be asked to provide information from the medical records of patients who are incapable of giving consent, are aged under 18 or have died to agencies external to the Trust. The groups that you need to be aware of and who will need to be considered when looking share personal data for non-direct care purposes are:

- **Children and young people with capacity -** Many young people have the capacity to consent to the disclosure of their medical records. If the child or young person (under 18 years of age) is able to understand the purposes and consequences of disclosure (Gillick competent) they can consent or refuse consent to the disclosure. You should discuss disclosing the information with them and release it only with the child or young person's consent. Where the information is required and without it may cause a patient/clinical risk, the information will be shared. In these cases it is required for direct patient care and gaining consent is not applicable.

- **Safeguarding children and young people up to their 19th birthday** - If a child or young person aged under 19 years refuses to consent to sharing their information with external agencies, you should nevertheless disclose the information if this is necessary to protect the child, young person or someone else from serious harm, or if disclosure is justifiable in the public interest.

  The Children Acts of 1989 and 2004 and the statutory guidance, 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children and young people' (2010, HM Government) mandate the sharing of information in this situation whether the child is with or without mental capacity, as long as the information shared is proportionate, appropriate and in the child's best interests.

  Examples include situations where you consider that the child or young person is at risk of neglect or abuse, the information would assist in the prevention, detection or prosecution of a serious crime, or where the child or young person may be involved in behaviour that might put themselves or others at risk of serious harm. It would also include a situation where a child or young person has refused to allow a carer to be told of a condition or treatment, from which there is a risk of a serious complication arising.

- **Children and young people without capacity** - The overriding principle, when dealing with the disclosure of the medical records of children or young people who do not have the maturity or understanding to make a decision, is ensuring that you act in their best interests.

  If the child or young person lacks the capacity to consent to the disclosure of information, those with parental responsibility can consent on their behalf. The consent of only one person with parental responsibility is needed for consent for disclosure.

If you do not believe that the decision made by those with parental responsibility is in the best interests of the child or young person, and the disagreement cannot be resolved with discussion and mutual agreement, it may be necessary to seek the view of the courts.

In young people aged 16-17 who lack capacity, both the Mental Capacity Act (MCA) 2005 and the Children Act 1989 can apply, depending on the circumstances. In England, the MCA defines anyone of age 16 and above as an adult. In relation to disclosure of information, the most important principle is to ensure that you are acting in the patient's best interests.

- **Adults lacking capacity** - Any disclosure must be justifiable and the reasons for doing so must be fully documented.

  The Mental Capacity Act 2005 applies to adults without capacity and further details about the disclosure of confidential information about a patient lacking capacity can be found in the Mental Capacity Act Code of Practice. Under the Act, patients are assumed to have capacity, unless they have an impairment affecting their mind (e.g. dementia), which means they are unable to make a specific decision at a specific time. There is also a requirement to ensure all practical steps have been taken to help the individual make a decision.

  The overriding principle is that the disclosure of confidential information is made in the best interests of the person lacking capacity. This may involve releasing information about their condition – for example to their carer, to ensure they receive the best treatment.

  If the patient has made a lasting power of attorney that covers personal welfare, you must consider the views of anyone who has legal authority to make a decision on the patient's behalf, e.g., a lasting power of attorney that covers personal welfare, or who has been appointed to represent them. Likewise, if the Court of Protection has appointed a deputy to make welfare decisions on behalf of the patient, that person must be consulted in relation to disclosures of confidential information.

Please contact the IG team who will be able to advise and let you know if there is another legal basis that can be applied.

### 7.4.4. Requests for Information on Patients or Staff

- Never give out information on individuals to persons who do not 'need to know.' Only if you have a justified reason and have been 'authorised to access' should this information be released, usually if involved in the patient's care for example
- Always check the identity of the person requesting the information
- Check the identity of telephone requesters by calling back using an independent source for the phone number
- All requests for identifiable information should be on a justified 'need to know' basis.
- Only the minimum necessary information should be given
- Follow existing 'Information Sharing Protocols'
- Some requests may need to be agreed by the SIRO, Caldicott Guardian or Trust procedures for example in the case of research
- If in doubt ask a health professional or your line manager or the IG Team

### 7.4.5. Requests for Information by the Police and Media

#### 7.4.5.1. Media

Do not release any personal data under any circumstances. All Media requests and calls should be referred to the Trust's Media, PR and Communications Department.

#### 7.4.5.2. Police

Requests for information from the Police should always be referred to the Legal Services department and where necessary they will liaise with Information Governance team who may further liaise with the SIRO and / or Caldicott Guardian if appropriate.

Under data protection legislation the police or other enforcing public agencies must provide a formal request for information under the Data Protection Act 2018 Schedule 2(1) and UKGDPR 6(i)(d). (This has replaced the previous Data Protection Act 1998 Section 29 (3) form).

This sets out the legal basis for the request, e.g. to assist in the prevention or detection of a crime, prosecution or apprehension of offenders, or those protecting the vital interests of a person. (Being a missing person is not a crime).

Note that it is still the Trust's decision as it remains the Trust's risk whether to disclose, it is not compulsory.

If the request is about any other matter or if in doubt contact the Legal Services Department before providing any information.

### 7.4.6. Disclosure of Information to other Employees of the Trust

Information concerning patients/staff should only be released to other staff members in the Trust if they have the access rights to that information, on a need to know basis and always:

- Check they are who they say they are via their ID Badge or internal extension number
- Check employees have a justifiable need to access the information
- Do not be bullied into giving the information

If in doubt, check with the person in charge of the individual's care or your manager.

### 7.4.7. Disclosure after a patient's death

Your duty of confidentiality extends beyond the patient's death. However, there may be circumstances when disclosure may be justified. For example, you are under a professional duty to respond to complaints, and this includes complaints made by bereaved relatives. Any disclosure must be justifiable and the reasons for doing so must be fully documented.

There is a Death Notification Procedure for all child deaths up to age 19 years that occur on Trust premises undertaken by the Paediatric Health Visitor Liaison team within the Trust who notify all relevant agencies within the region according to regional procedure on the first working day following the death. This Death Notification Procedure can be found in the Paediatric Health Visitor Liaison's Standard Operating Procedures.

All child and infant deaths and deaths as result of a domestic homicide, irrespective as to whether they occurred within the Trust are subject to a Serious Case Review led by the deceased's respective Local Authority. If the deceased is known to the Trust, the Trust via the Adult or Children's Safeguarding teams is required to share detailed information in an Individual Management Review signed off by the Trust's Executive Lead for Safeguarding. The review can

involve sharing information as part of the review process about the victim and other family members as requested by the leading authority. The Trust's Individual Management Review Completion Standard Operating Procedure can be found in the Trust's Safeguarding Children Policy and Standard Operating Procedures.

All sudden unexpected deaths in infancy (SUDI) and in children (SUDC) are subject to review by the Merseyside regional SUDI and SUDC protocols that require all agencies to share information. The SUDI and SUDC procedures are available in the Trust's Safeguarding Children Policy and Standard Operating Procedures.

Any request to disclose information for a Coroner's Inquest should be coordinated by the Trust's Legal Department. Trust staff asked to produce statements and reports for a Coroner's Inquest should submit their report/statement through the Trust's Legal Department and retain a copy themselves.

**Who can you disclose information to?**
You should consider whether disclosure would be justified in all the circumstances of the case.

The Access to Health Records Act 1990 applies to records of deceased patients, and to information recorded in or after November 1991. Under the Act, upon request, relevant information should be disclosed to the personal representative of the deceased (the executor of the deceased's will or the administrator of the estate if your patient died without leaving a will) or anyone who may have a claim arising from the patient's death.

If the request for disclosure is made by someone other than the personal representative or a person with a potential claim arising from the patient's death, then, where possible, you should advise them to seek the consent of the personal representative. If this is not possible you should consider whether disclosure would be justified in all the circumstances of the case.

**What information can be disclosed?**
If the patient has asked that specific information remains confidential, their views should be documented, and respected, subject to disclosures that are required by law or justified in the public interest. However, even in circumstances where you are not aware of any specific requests from the patient, there are factors you should take into account before disclosing any information:

- Is it information which, by its nature, the patient might not have wanted disclosed?
- Could the disclosure of the information cause serious harm or distress to others?
- Would the disclosure inadvertently reveal information about a third party?
- Is the information already in the public domain?
- Is the disclosure necessary?

## 7.5. Transfer of data

### 7.5.1. Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be:

- Specifically addressed to a named recipient never to a department, or a unit of an organisation
- Written communications containing personal data should be transferred in a sealed envelope and addressed by name to the designated person within each organisation.

They should be clearly marked “Personal and Confidential to be opened by the recipient only”
- The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale
- If an organisation has a policy that all mail is to be opened at a central point this policy must be made clear to all partners. An alternative means of transfer should be arranged where it is essential that the information is restricted to those who have a need to know
- The personal data contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role

**Internal** mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. ‘Confidential’ or ‘Addressee Only’, as appropriate.

**External** mail must also observe these rules. Special care should be taken with personal data sent in quantity, such as case notes, or collections of patient records on paper or removable media. These should be sent by Special / Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor. Personal data or data that is deemed sensitive to the Trust must not be sent to or from staff or third party personal email accounts, e.g. – Gmail, Hotmail etc.

**Electronic and removable media** must not be used without prior approval from the Director of Informatics or suitably authorised deputy and must be encrypted to NHS standards (contact the IT Service Desk) and should only be sent by recorded delivery or by the Trust approved courier service. Advice on how to password protect files is available via the IT Service Desk.

**Case notes** and other bulky material should only be transported in approved boxes and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless stored, waiting for collection, in a secure area e.g. ideally locked. The containers should only be taken and transported by the approved carrier.

### 7.5.2. Faxing

**Use of Fax Machines banned in the NHS from 1st April 2020**

From **April 2020**, NHS organisations were required to use modern communication methods, such as secure email, to improve patient safety and cyber security. This was part of the Health and Social Care Secretary’s tech vision, to modernise the health service and make it easier for NHS organisations to introduce innovative technologies. The Trust is working to remove all fax machines as it recognises one of the most common breaches of confidentiality occurs when documents that contain personal data are sent by fax machine. Many fax machines are in corridors or open plan offices and are used by several different departments. Staff collect faxes but do not always check that all the pages belong to them; this increases the risk of information being seen by unauthorised persons.

To combat this, the Trust has identified certain fax machines as ‘Safe Haven’ machines (refer to section 7.10 for more information on Safe Haven). These are machines that are located in a secure area and are used to receive documents of a private and confidential nature. Staff must contact their line manager for details of their nearest safe haven fax machine and a front cover sheet must be used.

Recipient fax numbers should be pre-programmed into fax machines and regularly checked. If this is not possible the recipient's fax number should be rechecked before the send button is pressed. Always remove information from the machine immediately after sending or upon receipt, and confirm receipt with the recipient. When faxing person identifiable information, follow Trust guidance located by fax machines.

### 7.5.3. Email

**Personal identifiers should be removed** wherever possible, and only the minimum necessary information sent; this may be considered to be the NHS number but no name or address. This in itself can pose problems as the wrong number may have been used. An individual's name should not be included in the subject line of an email; however, initials are permitted.

Special care should be taken to ensure the information is sent only to recipients who have a 'need to know'; always double check you are sending the mail to the correct person(s).

Where you do need to send personal data via email please check with your manager that you are allowed to do so. Any emails containing personal identifiable data or sensitive data must be placed in a password protected Word or excel document.

The document should then be attached to the email. It is vital that staff remember to ask the person receiving the email to phone the sender when received for the password. The password must not be included in the email. This is to safeguard you if the email is sent to the wrong address.

**External transfers** of personal data should only take place to persons with access to a secure account compatible with nhs.net. If a recipient does not have a recognised, secure e-mail account, use of the NHS Mail [Secure] function should be considered. In exceptional cases it may be necessary to email person identifiable information or sensitive or confidential information to persons who only have Internet access. In such cases the potential risk of loss and the insecure nature of using the Internet should be explained and communicated to the intended recipient and their agreement recorded.

If you are sending the email from a @sthk.nhs.uk address to any of the following it does not require encrypting;

| | | | |
|---|---|---|---|
| 5bp.nhs.uk | hsthpct.nhs.uk | onehalton.org.uk | sthk.nhs.uk |
| GP-N81066.nhs.uk | knowsley.nhs.uk | shk.nhs.uk | sthkhealth.nhs.uk |
| haltonccg.nhs.uk | knowsleyccg.nhs.uk | sthelens.nhs.uk | wbhospice.org.uk |
| haltongp.nhs.uk | knowsleypct.nhs.uk | sthelensccg.nhs.uk | willowbrookhospice.org.uk |
| his.sthk.nhs.uk | nwbh.nhs.uk | sthelenspct.nhs.uk | wshospitalscharity.org |

If you are sending from a @sthk.nhs.uk to any other email addresses it must be encrypted.

Sensitive personal information that identifies a service user or member of staff, or commercially sensitive information must not be sent by e-mail (.nhs.uk) unless it is encrypted to NHS standards.

After attaching your password protected document just simply type [ENCRYPT] in the subject line of the email and the system will enforce encryption. The person receiving the email will then be required to register to use the system with their email address. The process will take them approximately 90 seconds. Remember to ask the person receiving the email to phone you when the email is received for the password.

**Staff must never send personal data to any personal email address.**

**Staff must never send personal data from their personal email account to their Trust email account.**

The amount of time that an employee may use the e-mail system for reasonable personal use should be agreed with their line manager.

Copyright in all documents created via e-mail is the property of the organisation and not the individual user.

E-mails sent by a Trust employee are the organisation's property. Unless such e- mails are marked Personal in the 'Subject Field' they may be opened by the Trust.

E-mail (unless marked Personal in the subject field) is considered corporate correspondence and as such is accessible under the Freedom of Information Act 2000. It is therefore important to save e-mails that have been used to formulate corporate decisions, policy, or procedure, as they may be subject to a request. These e-mails should be referenced, saved and retained to appropriate record retention periods following advice from the organisation's Head of Information Governance.

Employees must not share their password and user name with any other person and should not leave their computers unattended whilst logged on, as they will be held responsible for any activity, which takes place using their account.

Unauthorised use of someone else's identity to send or intercept e-mail is strictly forbidden and will result in disciplinary action.

Employees must not distribute any material by e-mail which is:

- unlawful
- objectionable
- causes offence, examples of which include but is not limited to offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability
- contains material which is libellous or pornographic, includes incitement to commit a crime, hatred and violence or any activity that contravenes any of the Trust's Policies including Equal Opportunities Policy
- Material that could be abusive, indecent, obscene, menacing, or in breach of confidence, copyright, privacy or any other rights

Any member of staff who receives e-mail containing material which is in breach of this policy should inform their line manager immediately, who will instigate the organisation's incident reporting procedures.

Distribution of such material may result in legal action and/or disciplinary procedures. The Trust reserves the right to monitor e-mail usage.

Where a member of staff receives e-mails from unsolicited sources the sender should be added to their personal 'Blocked Sender List'. (Contact the IT Service Desk for information).

Where there is any doubt about the origin of an email or its attachments staff must contact the IT Service Desk for advice as viruses can be spread through e- mail and the opening of suspect attachments may result in loss of or damage to the Trust IT systems.

Users should exercise caution when disclosing their work e-mail address to commercial organisations, as this information may be passed to other 3rd party organisations generating 'junk' mail.

Employees must not use the organisations e-mail system to conduct any personal business enterprise.

It is inappropriate to forward or create chain letters to other e-mail users either within the organisation or externally. If a user receives a chain letter that has inappropriate content they must inform their line manager who will instigate the organisation's reporting procedures. Staff must also ensure that they do not click on links and attachments, from people they do not know, or that are contained within SPAM emails.

To avoid inappropriate content being circulated users should not set their e- mail to "auto forward" (Contact the IT Service Desk for information).

Only those employees who are specifically authorised to give media statements on behalf of the Trust, i.e. the Media, PR and Communications Department, may write or present views, concerning the Trust and its business, via e-mail.

Refer to Appendix C for information on Email Etiquette.

#### 7.5.3.1. E-mail – Monitoring

The Informatics Department retains copy of all internal and external e-mail which is received or sent. The Department will not use this facility to monitor individual employees e-mail traffic without written permission or unless they have a justified need to monitor or investigate an employee's e-mails.

The Informatics Department will investigate inappropriate activity on behalf of the Trust under the following circumstances:

- A report of or concern raised about the contents of a computer
- A report of inappropriate or unreasonable personal use of e-mail or the internet
- Routine monitoring identifies potential inappropriate use
- This list is not exhaustive

The Informatics Department reserves the right to carry out detailed inspection of any IT equipment without notice, where inappropriate activity is suspected. A more detailed investigation may involve further monitoring and examination of stored data including staff deleted data held on servers, disks, drives or other historical/archived material.

Access to the content of a member of staff's mailbox in their absence, other than for the monitoring purposes already referred to, will only be granted on submission of a written request from a Senior Manager of the Trust area concerned to the Informatics Service Desk for approval by the Information Security Team. This request must identify the business need for the access requested and indicate the mail message(s) required.

In the event of a user being absent from work for an extended period of time, access to their inbox may be granted to their line manager. The Informatics Department has a structured level of governance regarding granting access to e-mail records. Ultimate responsibility for this lies with the SIRO; when absent this responsibility is passed to the Deputy Director of Informatics.

The Informatics Department will only initiate a request for access to an individual's mailbox when a request for this access has been made in writing from the Senior Manager via the IT Service Desk to the Information Security Team.

### 7.6. Internet Access & Monitoring

Access to the internet or external web resources will be authenticated by user name and password.

The time of day that staff may use the internet for reasonable personal access should be agreed with their line manager but as a general rule staff should not exceed their agreed break times for non-work related Internet browsing.

Internet users must be aware that the internet is inherently insecure and confidential information in relation to the business of the Trust and/or service user/another staff member's identifiable information must never be disclosed or placed on internet sites or chat rooms. Although the Informatics Department has put anti-virus defences in place, great care should be taken when using the internet. The IT Service Desk should be informed where any suspicion of virus infection arises; the incident will be dealt with in accordance with information security procedures.

Downloading or distribution of copyrighted material without permission of the copyright holder, or of software for which the user does not have a legitimate license, is forbidden, this applies to any download for work or personal use.

The installation of downloaded software onto Trust computers, including laptops, is not permitted. The Informatics Department should be contacted for the installation of any required software. Information downloaded for personal use must not be stored on the Trust Network.

The use of computers connected to other networks (including peer-to-peer networking systems) to download files or software is forbidden as is the installation of any such system or software on Trust computers.

Access to the internet is authenticated and logged on a user basis. Details such as the date and time of access, and the site visited, are recorded and the information is retained for one month and then archived. Further reports will be available for use when investigating an incident; these reports will only be disclosed upon receipt of a written request from the Service Director in question.

### 7.7. Social Networking Sites (and Blogs)

Access to social networking sites, examples of which are Facebook, Twitter, Instagram and Snapchat (this list is not exhaustive) is strictly prohibited from Trust owned/managed computer equipment unless approval has been given by the SIRO to utilise social networking sites for the purpose of either communications or public information or to improve patient care.

Access to social networking sites will only be considered for approval once a request has been made in writing from the Service Director to the SIRO directly.

Staff must be aware that social networking sites make personal information publicly accessible, allowing people to upload to a profile with personal details, photos, videos and notes and to then link with their “friends” profiles. This raises immediate concerns about privacy.

Although individuals may believe they have restricted access of their profile to their “friend” list, the High Court ruled that all postings to social network sites are regarded as being in the public domain and as such potentially accessible to all.

Personal use of social networking sites may:

- Bring the organisation into disrepute by the posting of damaging remarks whether about the Trust, patients, service users, colleagues or other 3rd parties
- Give rise to risks of legal claims against the organisation, which is generally vicariously liable for the actions of its staff
- In line with BMA and GMC best practice guidance, staff should not ‘friend’ patients on Facebook, or any other social networking site

As a consequence of inappropriate use of social networking sites staff might find themselves:

a) Breaching this Policy
b) Damaging the organisation’s reputation in such a way as to constitute a breach of an individual’s employment contracts, leading to disciplinary action and possible dismissal.
c) Breaching confidentiality, data protection, employment contract or professional Code of Practice

It is therefore vital that staff who access or are members of social networking sites in a private capacity do not post images that have been taken inside of, in the grounds of, or on Trust premises, or place misleading, malicious, or derogatory comments or references that would damage the reputation of, or misrepresent the Trust, or cause distress to its patients, service users or any other staff.

Failure to comply will result in disciplinary procedures.

Staff should be aware that the Trust monitors information posted about the Trust online (both generally and on social media sites) for content that it finds inappropriate or any associated breaches of this policy.

Please refer to the Trust's Social Media Policy for more information.

### 7.8. Acceptable Personal Use of Email and Internet & Disciplinary Procedures

The Trust allows limited personal use of the e-mail and internet system.

The Trust considers that staff may browse the internet or use e-mail within the boundaries of this policy for their own personal use prior to or after their normal working hours or during their lunch or official break.

Where there is a necessity to conduct such activities within working hours this should be agreed with your line manager.

The time of day that staff may use the internet for reasonable personal access should be agreed with their line manager but as a general rule staff should not exceed their official breaks for non-work related Internet browsing.

Any misuse of social networking sites which has a negative impact on the Trust - including what might be perceived as online bullying and harassment – may be regarded as a disciplinary offence.

The use of racist, homophobic, sexist or other prejudicial language by staff, including in e-mails or on the internet may also be regarded as a disciplinary offence. Staff should ensure they follow the Respect & Dignity at Work Policy when using Social Media sites.

### 7.9. Passwords

#### 7.9.1. Password Protection

Personal passwords issued to or created by staff should be regarded as confidential and those passwords must not be communicated to anyone.

Staff will be given more information about password control and format etc. when receiving their training and/or password.

It is an NHS requirement for encryption to be applied to all Trust devices. To ensure the security of data held on mobile devices including access to NHS Mail accounts, staff must not store their passwords and/or pin numbers alongside any Trust devices issued to them e.g. a sticker containing a mobile pin code attached to a mobile phone case or writing passwords and pin numbers down in a notebook kept with a laptop or mobile phone.

No member of staff should attempt to bypass or defeat the security systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempts to breach security should be immediately reported to the IG Team and may result in disciplinary action breaches the Computer Misuse Act 1990 and/or the Data Protection Act 2018.

- Users must always ensure passwords:
    - Are a minimum of 9 characters in length
    - Contain at least three of the possible character types
    - Are changed at least every 90 days
    - Not reused within 24 months
    - Are changed on first login where a new password is issued by IT
    - Are secure and that no-one is able to see what is being typed in

Staff should be aware they must comply fully with this policy.

- Users must not:
    - Set a password that contains all or part of the username, your date of birth or any consecutively repeated characters
    - Write your password down on paper, a sticker or post-it and stick it under your keyboard or attach it to your screen. Diaries or notepads are also not a secure place to store passwords
    - Store passwords on mobile phones/tablets as they are not a secure place to store passwords & account information (they are easily stolen, most are not encrypted and do not have a PIN/Password set)
    - Share passwords as the audit trail is compromised- i.e. if the user recorded against a transaction (for example the update of the allergies field in a person's medical record) is not the stated specific individual, then exactly who made the transaction cannot be determined. This is important when considering legal challenges to data records- i.e. in the instance of potential legal proceedings

In exceptional circumstances the length of the password characters will be reduced to a minimum of four. This will have to be approved by the Director of Informatics as SIRO or their deputies.

If you discover someone is not complying with this policy you must report it directly to your line manager or to the Trust Information Security Team.

Systems owners may remove your access to their systems if you are found in breach of this policy which may impact your ability to do your job.

### 7.9.2. Single Sign On (SSO)

The Trust utilises a single sign on solution which can automatically manage backend passwords enabling them to be set to the maximum length and complexity possible for each system. As these passwords are never known to the users this in turn will make the individual systems more secure. This functionality will be implemented with the rollout of Single Sign On.

### 7.9.3. Account creation & resetting of passwords

Line managers must complete a login request form on the intranet for new starters detailing the systems and files they require access to, and the level of access.

IT Services will create an active directory account for the user after receipt of the new starter form from HR and on receipt of the login request form from the line manager. The username will be sent out by email to the line manager. The password will be given to the user over the phone when they start and staff are prompted to change it the first time they log on.

Please note that the above only relates to accessing the Trust Network and specific systems such as EDMS, PAS etc. Such system specific access will only be granted upon the completion of the relevant documentation and training.

If a user has forgotten their password or their account has been locked out, then the user should contact the IT Service Desk (Account reset queries should only be made by the person who the account belongs to). Checks will be made to verify that the user is who they say they are and

then the account can be unlocked or the password reset. Again the password will not be sent out in a message in clear text. Acceptable proof of identity can be the answer to a security question, or the service desk can contact switchboard and ask to be put through to the main departmental number and passed over to the user.

Users with single sign on can reset their password at the logon screen by answering three of the five security questions they answered when enrolled in the single sign on software.

All systems and applications (where possible) will be set up so that users will be forced to change their password at first time of logon after the creation of a new account or a password reset.

### 7.9.4. Generic passwords/accounts

Generic accounts are **not permitted within the Trust except** in exceptional circumstances and it is unavoidable (root & administrator accounts for example.)

Where possible these accounts will be subject to stricter password expiry rules, however a procedure must be in place so that when passwords are changed, users of these accounts are made aware (in a secure manner) and the old password is not entered, potentially locking the account.

## 7.10. Process for Safe Havens/Locations/Security Arrangements

When confidential information is received to a specific location in the Trust:

- It should be to a room/area that is lockable or accessible via a coded key pad known only to authorised staff
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors
- Ground floor rooms/areas must have lockable windows
- The room/area should conform to health and safety requirements in terms of fire, flood, theft or environmental damage
- Manual paper records containing personal information should be stored in locked cabinets when not in use
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use
- Equipment such as fax machines should have a code password and be turned off out of office hours, (if possible)

In Summary; Safe Haven procedures should be in place in any location where large amounts of personal information is being received, held or communicated especially where the personal information is of a sensitive nature e.g. personal data.

## 7.11. Cloud Storage Use

Cloud storage and file sharing website such as Dropbox are not allowed to be accessed due to the security and governance risks associated with these services. The Trust does not have the security mechanism and controls to safeguard information stored on Dropbox, or similar ‘cloud’ storage solutions; uploading personal/sensitive information on cloud storage services such as Dropbox puts the organisation’s data at risk and exposes the organisation and its operation to:

- Malicious files

- Identity theft
- Blackmail
- ICO Penalties

Access to cloud storage is only permitted with specific authorisation and approval from the SIRO or equivalent.

### 7.12. Capturing Images of Patients and Staff

Images of patients and of staff must not be taken on personal cameras, computers or mobile phones by any staff member or visitor. Doing so seriously risks breaching patient and staff confidentiality and the consent process, as well as breaching the law on data protection and human rights

If you need an image for clinical reasons for a patient, contact Medical Photography or X- ray out of hours.

### 7.13. Patient Capturing Images

The use of personal cameras, including camera and recording facilities on personal mobile devices, by patients is strictly forbidden on Trust premises unless the patient has the explicit approval of a senior member of staff (ward manager or equivalent), as this could in inadvertently breach patient confidentiality.
Under no circumstances are cameras or such devices with that facility allowed in secluded areas such as toilets, bathrooms and treatment rooms.

The Trust realises there will be certain occasions were patients would like to use their personal devices to record images, such as in maternity. In order to do so in a safe and secure environment the patient must seek the approval from a senior member of staff before capturing an image.

Personal cameras, including camera facilities on personal mobile devices, must not be used for any clinical purpose nor must they be used for the storing of clinical images however the clinical images were captured. Only camera equipment purchased by the Trust specifically for clinical use may be used.

### 7.14. Removable Media/User Disks/USB Devices/ CDs & DVDs

Removable media can be defined as any portable device that can be used to store and move information. Media devices can come in various formats, including:

- Universal serial bus (USB) memory sticks (also known as flash drives)
- Compact disks (CD)
- Digital versatile disks (DVD)
- USB hard disk drives
- Secure digital cards
- MP3 / MP4 players i.e. iPODs or any other brands
- Laptops, – iPADS, etc.
- Some mobile phones and digital cameras
- Dictation devices

The IT Service Desk must be contacted to clarify the use of any other media devices not listed above.

Anything you can copy, save and/or write information to which can then be taken away and transferred or read on another computer, must NOT be used on Trust equipment, unless prior authorisation from the IT Service Desk has been given.

The above access and monitoring of such devices will be managed by authorised software. Any databases other than legitimate Trust systems that contain patient/member of staff/ identifiable information should be password protected and should only be accessible to those who have been authorised to do so and should be kept on a secure 'drive'. Authority must be obtained from the IG Team to keep personal data on a database other than approved system databases.

### 7.15. Home working

It may be necessary for staff to work at their own home. If you need to do this you would first need to gain approval from your manager. If they agree, you would need to ensure the following are considered and remember that there is personal liability under the Data Protection Act 2018 and your contract of employment for breach of these requirements:

- Service user or staff manual records may not be removed from the Trust site(s) without managerial consent. If records contain personal data approval will be required by the SIRO. If approval is given please ensure there is a record that you have these records, where you are taking them to, the purpose for taking them and when they will be returned. This is particularly important for records that may contain sensitive data, for example patient/staff records
- Make sure when travelling home after collecting manual records or equipment, that they are put in the boot of the car out of sight (ensuring that the vehicle is locked when unoccupied) or carried on your person while being transported from your workplace to your home
- Remote access into networked services must be strongly authenticated using a Trust remote access token (VPN) or should be via an allocated Trust device i.e. laptop which would have been through IT security checks. Contact the IT Service Desk for further advice
- Ensure any personal information in portable electronic form is encrypted to prevent unauthorised access. If you need to transport data in this way you will need to speak to the IT Service Desk and the SIRO will be asked to approve the request
- While at home you have personal responsibility to ensure any records you may access are kept secure and confidential. You must not let any unauthorised person have any access to the records. This means that other members of your family and/or your friends/colleagues/visitors/contractors must not be able to see these records or affect any access in your absence
- Printing is not generally permitted while working at home. If you feel you need to print, approval must be gained from your line manager and a risk assessment completed. Each case will be assessed individually and the SIRO will decide whether the printing can be approved
- If you work with any service user or staff records on portable electronic media you must ensure all of the above apply. In addition you must ensure such information is effectively deleted when you have finished your work. See the Trust's Mobile Working and IM&T security policies for further details
- When returning the records to work the same procedure must be carried out, as above.
- Laptops containing personal data must be secured at all times, especially in transit. This will need clearance from the SIRO

- Any loss of records or data bearing media, such as laptops, must be reported immediately to your line manager as soon as the loss is known and reported via Datix. If appropriate the police should also be informed
- If you need to make any calls that are classed as confidential or may discuss patient / personal data please make sure you conduct these in a quiet area of the house and at an appropriate time, where it is unlikely your conversation may be overheard. Please keep personal data to a minimum when discussing in meetings or on calls

### 7.16. Abuse of Privilege

It is strictly forbidden for any member of staff to look, copy, download or make any unauthorised use of any clinical or personnel information relating to their family, friends, patients or people in the public eye, who are treated or employed by the Trust. Access to clinical, information is only acceptable if you are directly involved in the clinical care of a patient. This includes clinical records, photographic or x-ray images or any other information held in any other media appertaining to the care of a patient/or employee of the Trust. Any member of staff found to be in breach of this principle will be subject to the Trust's disciplinary procedures and may be subject to Civil Action in the case of Data Protection breaches.

In cases where a close friend, partner/spouse or relative is, or becomes, a service user/patient, it is the responsibility of the employee to inform their line manager that such a relationship exists. The line manager will discuss the situation with the employee and agree an appropriate course of action. It may be appropriate for the service user/patient to be treated by another clinician or team, or, in the case of an inpatient admission, for the employee to be moved to another area for the duration of the service users/patient's treatment.

Staff must not access the service user records, as this will be classified as non-authorised access to clinical records and will be considered a breach of Trust policy, which could result in dismissal in accordance with the Disciplinary Policy.

Staff should not attempt to bypass or defeat the security systems attached to Trust systems or attempt to obtain or use passwords or privileges issued to other employees. Any attempt to breach the security of Trust electronic systems should be immediately reported to the Information Security Officer and would be considered a breach of the Computer Misuse Act 1990, Police and Justice Act 2006 Privacy and Electronic Communications Regulations 2003 and/or the Data Protection Act 2018.

### 7.17. Carelessness

- Do not talk about patients in public place, or where you can be overheard
- Do not leave any medical records or confidential information lying around unattended
- Make sure that computer screens are not visible to the public or facing windows
- Always lock your computer screen if you leave it unattended – by pressing the Windows key (bottom left of your keyboard) and the 'L' key together
- Whiteboards/chalkboards should not display any personal data
- Clinic lists should not be left in rooms especially those accessible to the public
- Remove all paperwork used in meetings from the room after use
- Do not pin any patient lists or documents on walls
- Personnel/staff records should be kept in a locked room and locked cabinet

### 7.18. Reporting Data Breaches

Staff should read this in conjunction with the Incident Management Reporting Policy and the Data Security and Protection Breaches Policy and Procedure. Staff should be aware of their responsibility to report any breach or risk to the confidentiality and/or integrity of information that they become aware of as outlined below:

- Report breaches to your line manager and through the Trust Incident Management Reporting Procedures (Datix). If you feel that it would compromise your position you may report the breach, confidentially, directly to the IG Team
- Once a Line Manager has been notified of a breach they should report the incident immediately to the Information Governance Team via Datix, giving details of the breach, date, time, place and any other relevant information
- Report any inadequate procedures that might lead to a breach
- There is specific legislation to protect individuals reporting any breach (contact the Human Resources department for further information). When dealing with a suspected or actual breach of information governance, staff should refer to the IG Team
- Suspected breaches of personal data must be reported to the IG Team. Confidential reports of suspected breaches may be made via the Trust's Protected Disclosure of Issues of Concern Policy (Whistle-blowing)

### 7.19. Non Compliance

Non-compliance with this code of conduct by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust disciplinary procedure, and may lead to dismissal for gross misconduct (Disciplinary Policy and Procedure).

Examples of failure to comply with confidentiality responsibilities include, but are not limited to, deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal/sensitive information electronically without encrypting it, etc.

## 8. Training

Information Governance knowledge and awareness is at the core of the organisation's objectives, without this the ability of the organisation to meet legal and policy requirements will be severely impaired.

To ensure organisational compliance with the law and central guidelines relating to Information Governance all staff are mandated to complete annual IG training. The Trust will ensure that all staff and workers are provided with the necessary security guidance, awareness and appropriate training to discharge their data protection and information security responsibilities. Those staff who have additional responsibilities within their role may be required to undertake appropriate additional modules as identified in the Information Governance Training Needs Analysis (TNA).

All staff and workers will be made aware of the contents and implications of this Information Governance and (where appropriate) information security procedures as irresponsible or improper actions by users may result in disciplinary action(s).

## 9. Monitoring Compliance

The Trust will conduct year-on-year assessments and develop improvement plans by:

- Monitoring its compliance with Information Governance Framework by completing a yearly assessment and attaining the standards within the Data Security and Protection Toolkit (DSPT)

- Undertaking or commissioning an independent assessment or audit of the DSPT requirement in line with the DSPT audit framework
- Providing assurance to the Trust board via the Information Governance Steering Group and the Risk Management Council after reviewing and agreeing annual reports and proposed actions/development plans arising from the DSPT

The table below outlines the Trust's key performance indicators and monitoring arrangements for this Policy. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

### 9.1. Key Performance Indicators (KPIs) of the Policy

| No | Key Performance Indicators (KPIs) Expected Outcomes |
|---|---|
| 1 | Duties are carried out as described in the Policy |
| 2 | Compliance will be monitored via the DSPT |
| 3 | External Audit Rating to be of an acceptable standard |

### 9.2. Performance Management of the Policy

| Minimum Requirement to be Monitored | Lead(s) | Tool | Frequency | Reporting Arrangements | Lead(s) for acting on Recommendations |
|---|---|---|---|---|---|
| Duties are carried out as described in the policy | IG Manager and DPO | Audit | Annual | IG Steering Group | IG Manager and DPO |
| Compliance will be monitored via the DSPT | IG Manager and DPO | DSPT Submission | Monthly | IG Steering Group | IG Manager and DPO |
| External Audit Rating to be of an acceptable standard | IG Manager and DPO | External Audit | Annual | Audit Committee | IG Manager and DPO |
| Information Governance Training | Training will be monitored in line with the Induction Mandatory and risk Management Training Policy. | | | | |

## 10.References

| No | Reference |
|---|---|
| 1 | UK General Data Protection Regulation 2018 |
| 2 | Data Protection Act 2018 |
| 3 | Freedom of Information Act 2000 |
| 4 | Environmental Information Regulations |
| 5 | Access to Health Records Act 1990 |
| 6 | Regulation of Investigatory Powers Act |
| 7 | Health and Social Care Act 2012 |
| 8 | Human Rights Act 1998 |
| 9 | NHS Code of Confidentiality |
| 10 | Caldicott Guardian Manual 2017 |
| 11 | NHS Information Risk Management |
| 12 | Records Management Code of Practice |
| 13 | Data Security and Protection Toolkit (DSPT) |

| | |
|---|---|
| 14 | Caldicott Reports |
| 15 | ICO Guidance |
| 16 | The Computer Misuse Act 1990 |

## 11.Related Trust Documents

| No | Related Document |
|---|---|
| 1 | IG Strategy |
| 2 | Information Governance Policy |
| 3 | Data Security and Protection Breaches / Incident Reporting Policy and Procedure |
| 4 | Corporate Records Management Policy |
| 5 | Freedom of Information Policy |
| 6 | Data Quality Policy |
| 7 | Registration Authority Policy |
| 8 | Network Security Policy |
| 9 | Back Up Policy |
| 10 | Mobile Device Policy |
| 11 | Remote Access Policy |
| 12 | Removable Media Policy |
| 13 | Disciplinary Procedures Policy |
| 14 | Equality and Diversity Policy |
| 15 | Harassment at Work Policy |

## 12. Equality Analysis Form

The screening assessment must be carried out on all policies, procedures, organisational changes, service changes, cost improvement programmes and transformation projects at the earliest stage in the planning process to ascertain whether a full equality analysis is required. This assessment must be attached to all procedural documents prior to their submission to the appropriate approving body. A separate copy of the assessment must be forwarded to the Patient Inclusion and Experience Lead for monitoring purposes. Cheryl.farmer@sthk.nhs.uk. If this screening assessment indicates that discrimination could potentially be introduced then seek advice from the Patient Inclusion and Experience Lead. A full equality analysis must be considered on any cost improvement schemes, organisational changes or service changes which could have an impact on patients or staff.

| **Equality Analysis** | | | |
|---|---|---|---|
| **Title of Document/proposal /service/cost improvement plan etc:** | Code of Confidentiality | | |
| **Date of Assessment** | 16/11/2021 | **Name of Person completing assessment /job title:** | Camilla Bhondoo |
| **Lead Executive Director** | Director of Informatics | | Head of Risk Assurance and Data Protection Officer |

| | **Does the proposal, service or document affect one group more or less favourably than other group(s) on the basis of their:** | **Yes / No** | **Justification/evidence and data source** |
|---|---|---|---|
| **1** | Age | No | No applies to ALL Staff |
| **2** | Disability (including learning disability, physical, sensory or mental impairment) | No | No applies to ALL Staff |
| **3** | Gender reassignment | No | No applies to ALL Staff |
| **4** | Marriage or civil partnership | No | No applies to ALL Staff |
| **5** | Pregnancy or maternity | No | No applies to ALL Staff |
| **6** | Race | No | No applies to ALL Staff |
| **7** | Religion or belief | No | No applies to ALL Staff |
| **8** | Sex | No | No applies to ALL Staff |
| **9** | Sexual Orientation | No | No applies to ALL Staff |
| | **Human Rights – are there any issues which might affect a person's human rights?** | **Yes / No** | **Justification/evidence and data source** |
| **1** | Right to life | No | Ensures staff comply with the law |
| **2** | Right to freedom from degrading or humiliating treatment | No | Ensures staff comply with the law |
| **3** | Right to privacy or family life | No | Ensures staff comply with the law |
| **4** | Any other of the human rights? | No | Ensures staff comply with the law |

| **Lead of Service Review & Approval** | |
|---|---|
| **Service Manager completing review & approval Job Title:** | Camilla Bhondoo<br>Head of Risk Assurance and Data Protection Officer |

## Appendix A – Full Responsibility around E-mail and Internet Use

**Organisational Responsibilities**

- Establish adverse incident and investigation procedures for the reporting of all breaches of this policy through the appropriate management channels
- Ensure that line managers understand their responsibilities for the implementation of this policy within their business or clinical area and that their managed staff adhere to the principles
- Provide appropriate training on the acceptable use of e-mail and the internet
- Ensure that controls are in place to prevent unauthorised access to the computer systems that allow access to the e-mail and internet system
- Compliance with section 46 of the Freedom of Information Act Code of Practice on Records Management with relation to disclosure of e- mails
- Defining acceptable personal use of e-mail and the internet

**Caldicott Guardian Responsibilities**

- Ensure that the organisation is aware of key legislation relating to this policy
- Ensure that systems are in place to investigate breaches of this policy
- Guide the organisation on the transfer or disclosure of person identifiable information by e-mail and the internet

**Line Managers Responsibilities**

Line Managers must ensure that permanent/temporary staff, students, trainees and contractors working in their departments are aware of:

- This policy and related policies
- The acceptable personal use of e-mail and the internet
- How to access advice and guidance on e-mail and internet acceptable use
- The security of the physical environment in their department
- How to report breaches or potential breaches of the E-mail and Internet Policy
- Line Managers can request monitoring of e-mail or internet use of their staff following the principles set out in section 7.7.3.1
- Line Managers must ensure they set the acceptable use standards for their staff.
- Once a Line Manager has been notified of a breach of this policy they should report the incident immediately to the Caldicott Guardian or Information Governance Team via Datix, giving details of the breach, date, time, place and any other relevant information
- Any inadequate procedures that might lead to a breach should also be reported by the process set out above

**Informatics Responsibilities**

- Reviewing this policy in line with changes in legislation/guidance/standards
- Providing, managing, and maintaining the e-mail system and internet access
- Monitoring and auditing access (see section 7.5.3.1)
- Supporting the investigation of reported incidents
- Complying with legitimate requests for access to mailboxes (see section 7.5.3.1)
- Staff training on the acceptable use of e-mail and the internet
- Maintain the library of blocked URL categories
- Username and password management
- Virus control
- Reporting incidents and inappropriate use to the Board through the information Governance Steering Group
- Reporting on issues raised

- Disseminating this policy in the organisation
- Acting as a source of help, advice and guidance on the acceptable/unacceptable use of e-mail and the internet and the content of this policy
- Ensure that all consultants, executives and suitably authorised individuals have access to streaming video and social networking sites to assist in the conduct of their duties in line with this Policy
- Responsible for monitoring as described in section 7.5.3.1
- Monitor all e-mails that are sent externally in order to ensure staff are abiding by this policy. Monitoring will be to ensure compliance with this policy and in particular will be looking for e- mails containing patient/ sensitive /personal identifiable information. Where necessary, the Trust will contact individuals who are sending such information out inappropriately
- The Informatics Department will only initiate a request for access to an individual's mailbox or a restricted website, when a request for this access has been made in writing from the Service Director to the Assistant Director of ICT
- The Informatics Department will only initiate a request for access to individual's internet records, when the Assistant Director of ICT has received a written request from the Service Director of the Trust area in question

**Information Security Team**

The Information Governance Team will task the Information Security Team with performing all monitoring actions and report upon findings to the IG Manager as and when required.

**Staff Responsibilities**

- Comply with this policy at all times including any use of the service whilst off duty
- Report any incidents such as inappropriate use or security breaches or virus infection to their line manager
- Complete the signatory document in Appendix F after reading this policy
- Always ask for advice and guidance on the content of this policy or use of e-mail and the internet from line managers or the Informatics Service Desk if unsure of the content
- The Informatics Department has blocked certain inappropriate sites to prevent accidental access. Staff should not try to bypass security systems to try and access such sites
- If a staff member accidentally accesses material of the type referred to in the previous paragraph or other material which may be considered offensive, they should note the time and web site address, exit from the site and then inform their line manager who will instigate the Trust's reporting procedures
- Staff must not sell or provide non-Trust products or services or otherwise conduct non-Trust business via Trust provided internet access
- If a staff member is in doubt as to whether it is appropriate for them to access a site, they should speak to their line manager before doing so
- Only those staff who are specifically authorised to give media statements on behalf of the Trust may write or present views concerning the Trust and its business, on the internet.
- Staff must never access the internet using another individual's login. It is totally unacceptable to adopt a colleague's identity on any internet site
- Where an individual orders personal items from an internet site (for example, internet shopping) they must not arrange for them to be delivered to any Trust premises
- Staff must not download, upload, access or distribute any material whose subject matter is:
    a. Unlawful
    b. Objectionable
    c. Causes offence - examples of which are material which is libellous or pornographic or which includes offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability this includes incitement

of hatred or violence or any activity that contravenes the Law or the Trust Policies listed in section 11

d. Material that could be classed as abusive, indecent, obscene, menacing or in breach of confidence, copyright, privacy or any other rights.

- Confidential information in relation to the business of the Trust and/or service user/another staff member's identifiable information must never be disclosed or placed on internet sites or chat rooms
- Staff should inform the IT Service Desk where any suspicion of virus infection arises
- Staff must not download or distribute copyrighted material without the permission of the copyright holder, this applies to any download for work or personal use
- Staff should not download software onto Trust computers, including laptops
- Staff should not store downloaded information for personal use on the Trust Network
- Staff should not connect to other networks (including peer-to-peer networking systems) to download files or software, unless authorised to do so by the Deputy Director of Informatics, usually in cases where the service is required to in order to fulfil its obligations
- Staff who access or are members of social media sites in a private capacity must not post images that have been taken inside of, in the grounds of, or of Trust premises, or place misleading, malicious, or derogatory comments or references that would damage the reputation of, or misrepresent the Trust, or cause distress to its service users or any other member of staff
- Staff must not use a Trust e-mail address to sign up to social media sites for personal use
- When using social media for personal purposes, staff must not state or imply that they are speaking on behalf of the Trust. If confusion is likely to arise, staff may wish to use a disclaimer that clarifies things, for example 'these are my personal views and not those of my employer'
- Staff must not disclose any confidential information relating to the business of the Trust, to their employment at the Trust, to the employment of colleagues or relating to any staff members
- Staff must comply with all Trust policies when using social media, for example, you should be careful not to breach the Trust's Information Security Policy or Code of Confidentiality
- Sites must not be used to abuse other staff members, service users or volunteers. Privacy and feelings of others should be respected at all times
- Staff must consider carefully whether it would be appropriate to befriend someone when using social media for personal purposes where there is a professional/client/pupil relationship, and/or where this could create a potential conflict of interest
- Viewing and updating sites, blogs or other regular web presences used for purely personal purposes should not take place during working time (which excludes recognised breaks)
- If approached by a media contact about content on a site relating to the Trust, staff should immediately contact the Head of Media, PR and Communications for advice and support, following the existing policy
- Staff members should identify themselves as staff of the Trust only when appropriate
- Staff must not share their password and user name with any other person and should not leave their computers unattended and unlocked whilst logged on, as they will be held responsible for any activity which takes place using their account
- Unauthorised use of someone else's identity to send or intercept e- mail is strictly forbidden and will result in disciplinary action
- Staff must not distribute any material by e-mail which is:
    a. Unlawful
    b. Objectionable

c. Causes offence, examples of which include but is not limited to offensive material relating to gender, race, sexual orientation, religious or political convictions, or disability
d. Contains material which is libellous or pornographic or includes incitement to commit a crime, hatred and violence or any activity that contravenes any of the Trust's Policies including Equal Opportunities Policy
e. Material that could be classed as abusive, indecent, obscene, menacing, or in breach of confidentiality, copyright, privacy or any other rights

- Any member of staff who receives e-mail containing material which is in breach of this policy should inform their line manager immediately, who will institute the organisation's incident reporting procedures. Distribution of such material may result in legal action and/or disciplinary procedures
- Where a member of staff receives e-mails from unsolicited sources, the sender should be added to the receiver's personal 'Blocked Sender List' (The Service Desk can provide instructions on how to do this if required). The Informatics Department will occasionally review staff personal Blocked Sender Lists with a view to blocking e-mail from prolific unsolicited sources
- Staff who receive e-mail attachments, where there is any doubt about the origin, should contact the Service Desk for advice. Viruses can be spread through e-mail and opening suspect attachments may result in loss of data or damage to the Trust IT systems
- Staff must not use the organisation's e-mail system to conduct any personal business enterprise
- It is considered inappropriate to forward or create chain letters to other e-mail users either within the organisation or externally. If a user receives a chain letter they must inform their line manager who will instigate the organisation's reporting procedures. A chain letter is a letter which compels the receiver to forward the message to others, usually with the threat of adverse consequences if this is not done
- Chain letters sometimes contain warnings about virus outbreaks; these are often hoaxes which should not be forwarded or acted upon. If users are unsure as to the legitimacy of an e-mail they should forward this to the Informatics Department for investigation.
- To avoid inappropriate content being circulated and breaching the principles of the Data Protection Act 2018 and the UK General Data Protection Regulation, users should not set their e- mail to "auto forward"
- Staff must never send patient identifiable information to external e- mail addresses (which includes their personal e-mail address)
- Only those staff members who are specifically authorised to give media statements on behalf of the Trust, i.e. the Communications, PR and Media Department, may write or present views, concerning the Trust and its business, via e-mail
- Staff must never send patient identifiable information to their personal e-mail address
- If a user is unsure of any aspect of sending person identifiable information electronically, then guidance should be sought from the IT Service Desk
- Staff must follow the principles outlined in this policy on sending information securely
- The use of unapproved non-corporate deployed Instant Messaging (IM) clients and connectivity is strictly prohibited
- Staff may browse the internet or use e-mail within the boundaries of this policy for their own personal use prior to or after their normal working hours or during their lunch break as agreed with their line manager. This time period should not exceed 1 hour
- Staff should be aware of their responsibility to report any breach or risk to the confidentiality of information that they become aware of
- Staff should report breaches to their line manager and through the Trust Incident Reporting Procedures (Datix). If users feel that it would compromise their position they may report the breach (confidentially) directly to the Caldicott Guardian or Information Governance Manager

- Any inadequate procedures that might lead to a breach should also be reported by the process set out above

Users of the internet must be aware that each site they visit is recorded and logs of sites are regularly examined. Inappropriate usage may result in disciplinary proceedings. Information can be shared with the Local Counter Fraud Specialist and will be utilised in fraud investigations. A full security audit trail is maintained of records/sites accessed.

## Appendix B – Legal Implications of Email and Internet

**Email Legal Implications**

E-mail has been established as a means of communication for businesses and its use is now widespread. E-mail carries the same legal status as written documents and should be used with the same care. Several factors combine to make e-mail a particularly important issue within Government legislation.

- Where an e-mail contains personal data it will fall within the boundaries of the Data Protection Act 2018 and UK GDPR.
- When e-mail content relates to a living individual its disclosure may be required under the data subject's rights under the Data Protection Act 2018 and UK GDPR.
- E-mails may be subject to disclosure under the Freedom of Information Act 2000.
- E-mails that contain inappropriate comments may constitute breaches of Equality and Diversity or Disability Discrimination, Human Rights or other similar legislation.
- Sending emails that are offensive, abusive or harassing may constitute a criminal offence.
- E-mails are considered a form of publication and inappropriate comments may constitute libel contrary to the provisions of the Defamation Act 1996.

Misuse of e-mail and the internet may result in legal liability for the Trust and, in some cases, the individual user. Inappropriate use may give rise to:

- Liability for defamation
- Copyright infringement
- Breach of confidentiality
- Inadvertently entering into contracts
- Claims of harassment and discrimination
- Claims for compensation

**Social Media Legal Implications**

All Trust staff should bear in mind that information they share through social media, even if they are on private spaces, is subject to copyright, The Data Protection Act 2018, The Safeguarding of Vulnerable Groups Act 2006, The Computer Misuse Act and any other relevant legislation.

Although individuals may believe they have restricted access of their profile to their "friend" list or list of contacts, the High Court has previously ruled that all postings to social network sites are regarded as being in the public domain and as such potentially accessible to all.

It is critical that staff comply with this policy in their use of social media sites. Failure to do so will lead to their conduct becoming subject to investigation under the relevant Disciplinary Procedure.

Staff should be aware that there is an implied legal duty of trust and confidence between an employer and employee. It is possible therefore that any inappropriate use of social media both in or outside the workplace, for example by making unjustified negative comments or defamatory comments about the Trust, its clients, or staff, could result in disciplinary action if it brings the Trust's reputation into disrepute, or exposes the Trust to potential liabilities. The Trust recognises and upholds the right of staff to make public interest disclosures ("whistleblowing"- refer to the Raising Concerns Policy) when necessary but would not envisage that such disclosures could be justifiably made using social media.

**RIPA**

**The Regulation of Investigatory Powers Act 2000 (RIPA) & Telecommunications Act 2000**

Section 1 (3) of RIPA prevents interception of communications in the UK without lawful authority. The Trust considers all the information that it holds to be valuable and will strive to ensure that it is therefore handled in accordance with Trust Policy. In order to ensure staff are abiding by policy, the Trust will monitor all emails that are sent containing patient/sensitive /personal identifiable information externally and where necessary contact individuals who are sending such information out inappropriately.

Under the provisions of the Act, the proposed monitoring of emails would amount to "interception of communications". This interception of communications is rendered lawful as it is undertaken in compliance with the Telecommunications Regulations 2000. These Regulations talk in terms of "business practice" and business is defined as including activities of a public body such as the Trust (Regulation 2a).

Regulation 3 of the Regulations permits the monitoring and recording of communications without consent to establish the existence of facts relevant to the organisation which can include the need to:

- Ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business (such as compliance with the DPA regarding the disclosure of personal data via email)
- Ascertain or demonstrate standards which are or ought to be achieved by staff using the system
- Prevent or detect crime
- Investigate or detect the unauthorised use of the telecommunications system
- Ensure the effective operation of the system

To ensure the Trust is in compliance with the Telecommunications Regulations 2000, the Trust will have made all reasonable efforts to inform staff who may use email, that interception/monitoring of outbound emails, where personal data has been identified, will take place.

## Appendix C – Email Etiquette

- When sending messages or responding to messages sent by other users, your recipient might have different views, opinions and cultures. Without vocal inflection and body language, sarcasm, facetiousness and what you would consider innocent ‘fun’ can be misinterpreted as being rude or abusive
- E-mail messages should not be written in CAPITAL letters as this is considered to be aggressive or the equivalent of shouting
- The subject field should always be used to add a short description of the contents of the e-mail. This will assist the recipient in prioritising the opening of e-mail and will aid the retrieval of opened messages
- Care should be taken with content. You should never write anything in an e-mail that you would not write in a letter or say to someone face to face. You should also take into account that e-mail records can be permanent and can be disclosable
- The same conventions should be used as when sending a letter by post, e.g. using the same style of greeting
- E-mails should be signed off with the name, title and contact details of the sender. This can be added to a signature file so that it appears automatically (contact the Informatics Department for assistance with this if required)

## Appendix D – Caldicott Principles

**Principle 1: Justify the purpose for using confidential information -** Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

**Principle 2: Don't use personal confidential data unless absolutely necessary -** Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

**Principle 3: Use the minimum necessary personal confidential data -** Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

**Principle 4: Access to personal confidential data should be on a strictly need-to-know basis -** Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

**Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities -** Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**Principle 6: Understand and comply with the law** - Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

**Principle 7: the duty to share information can be as important as the duty to protect patient confidentiality** - As much as it is permitted to share information only in the best interest of the patient, an organisation must ensure it protects the confidentiality of the patient.

Sometimes, information might be needed by government agencies or research and development organisations for other purposes. In such cases, health and social workers should be able to share the information but must make sure that the patient is anonymous.

**Principle 8: inform patients and service users about how their confidential information is used -** Steps should be taken to ensure there are no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

## Appendix E – UK GDPR Lawful Basis

Where personal data is being processed a lawful basis set out in Article 6 of the UK GDPR must be applied:

**(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
**(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
**(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
**(d) Vital interests:** the processing is necessary to protect someone's life.
**(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. (Used for direct care)
**(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

In addition when processing special categories of data (formerly sensitive data) a condition from Article 9 of the UK GDPR must also be applied.

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

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.

Please refer to the IG Team for more information and guidance.

## Appendix F – Staff Signatory Page

**IM&T Information Security**
**Code of Confidentiality Acceptance Form**

I have been given a copy of and can confirm I have read and understood the content of the Trust's Code of Confidentiality.

I understand that I am bound by a duty of confidentiality and agree to adhere to the Code of Conduct at all times.

I understand that I must seek guidance from the Information Governance Team or my Line Manager if any part of this policy is not clear to me.

I understand that, by accepting my account password and related information and accessing the organisation's Network and Internet system, I agree to adhere to this policy.

I understand that I must report any network or internet misuse to my Line Manager or Information Governance Team.

I understand that I must follow the guidance in this document and must not breach any of the principles

I understand that if I let another person use my e-mail or internet account I will be held equally responsible for any violations of this policy that may occur

I understand that if I breach any of the principles and guidance in this policy or fail to report violations of these principles by other users that I may be subject to disciplinary action.

I consent to the monitoring of my e-mail and internet use for the purposes of ensuring my compliance with the Code of Confidentiality.

Signed……...
Print name…….
Date……

This signatory document will be kept on your personnel record to appropriate records' retention periods