NHS
South West
Yorkshire Partnership
NHS Foundation Trust

| | |
|---|---|
| **Document name:** | Data Security & Protection |
| **Document type:** | Policy |
| **What does this policy replace?** | Version 1.2 of this policy |
| **Staff group to whom it applies:** | Everyone who processes personal, confidential data |
| **Distribution:** | The whole of the Trust |
| **How to access:** | Intranet |
| **Issue date:** | February 2024 |
| **Next review:** | February 2025 |
| **Approved by:** | Executive Management Team<br>8 February 2024 |
| **Developed by:** | Information Governance Manager/ Data Protection Officer |
| **Director leads:** | Chief Nurse/ Director of Quality & Professions<br>Director of Finance & Resources |
| **Contact for advice:** | Information Governance Manager/ Data Protection Officer |

# Table of Contents


| | |
|---|---|
| 1 Introduction | 3 |
| 2 Purpose & Scope | 4 |
| 3 Definitions | 6 |
| 4 Duties | 11 |
| 5 Principles | 16 |
| 5.1 Responsibility of the Trust | 16 |
| 5.2 Principles relating to the processing of personal data | 18 |
| 5.3 Lawfulness of processing | 18 |
| 5.4 Processing of special categories of personal data | 19 |
| 5.5 Processing of personal data relating to criminal convictions & offences | 26 |
| 5.6 Duty of confidentiality | 26 |
| 5.7 Caldicott principles | 27 |
| 5.8 Rights of data subjects | 27 |
| 5.9 Security of personal data | 34 |
| 5.10 Other Trust information | 34 |
| 6 Equality impact assessment | 35 |
| 7 Dissemination & implementation arrangements | 41 |
| 8 Procedure for monitoring compliance & effectiveness | 42 |
| 9 Review & revision arrangements | 43 |
| 10 References | 44 |
| 11 Associated documents | 45 |
| 12 Appendices | 46 |
| 12.1 Appropriate policy document: data processing for the purposes of employment, social security & social protection | 46 |
| 12.2 Appropriate policy document: processing of special categories of personal data for reasons of substantial public interest | 49 |
| 13 Version control | 53 |

# 1. Introduction

The Trust's vision is to provide outstanding physical, mental and social care in a modern health and care system.

The Trust's mission is to help people reach their potential and live well in the community.

To deliver our vision and mission, the Trust must process personal, confidential data pertaining to patients, service users and staff.

Individuals have legal rights in respect of the personal data the Trust holds about them, and the Trust must have processes in place to enable individuals to exercise those rights.

The Trust recognises that appropriate levels of protection and security must be applied to its personal, confidential data to maintain its confidentiality, integrity and availably at all times.

This is a new, single policy that brings together the principles for processing personal data, individuals' rights and information security in line with current legislation and national guidance.

## 2. Purpose and scope

The primary purpose of this policy is to assure the Executive Management Team (EMT) that the Trust will use and share its personal, confidential data and protect the availability, integrity and evidential value and availability of its information, information systems and staff in line with:

- The principles, rights and security requirements set out in the UK GDPR
- The provisions for the regulation of the processing of information relating to individuals and to exemptions from the UK GDPR set out in the Data Protection Act 2018
- The provisions of the Access to Health Records Act 1990
- The standards set out in the Confidentiality: NHS Code of Practice
- The standards set out in the Confidentiality: NHS Code of Practice Supplementary Guidance on Public Interest Disclosures
- The standards set out in the Information Security Management: NHS Code of Practice*
- The requirements of ISO27001*

*Insofar as the scope of this policy allows (see areas outside scope below).

This policy will also assure the EMT that processing of confidential, personal data within the health and social sector for direct care and other purposes is in line with the National Data Guardian's:

- Caldicott Principles
- Data security and protection standards for health and social care

This policy covers all information held by the Trust, regardless of contact, format or media used to create and store it; and supersedes previous policies to create a single policy covering most aspects of data security and protection, including:

- Leadership, accountability and responsibility
- Individuals' rights, including the right of access/ subject access requests, the right to be informed and transparency
- Data sharing and data flow mapping
- Information assets, including consent and other lawful bases for processing
- Data protection by design, including data protection impact assessments
- Reporting personal data breaches

The following are outside the scope of this policy:

- Acceptable use of information technology
- Access controls (technical and physical)
- Cyber incidents and security
- Data quality assurance
- Freedom of Information
- IT security and protection
- Network security

- Records management (health and non-clinical), including data disposal

This policy applies to all individuals in the Trust who process personal, confidential data in the performance of the Trust's functions. This includes but is not limited to:

- Full and part time employees
- Non-executive directors
- Medical locum staff
- Students and trainees
- Secondees and staff on temporary placements from other organisations
- Volunteers
- Governors
- Visiting professionals and researchers
- Employees of other organisations who have approved access to Trust data
- Contracted third parties and agency staff
- Contracted organisations and companies providing support to the Trust
- Bank staff

Wilful or negligent disregard for the policy will be investigated and, where necessary, the Trust's Disciplinary and Capability Procedure will be followed.

# 3. Definitions

**Access to Health Records Act 1990**
Since 1998 when it was largely superseded by the Data Protection Act, the law that applies in England and Wales to provide access to the health records of the deceased to certain people in certain circumstances.

**Appropriate Health Professional (Data Protection Act 2018 schedule 3, part 2, section 1(1))**

- The health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matter(s) to which the data relates
- Where there is more than one such health professional, the most appropriate is the one most suitable to provide an opinion on the data in question
- Where there is no professional available that falls into either of the two definitions above, the most appropriate is a health professional who has the necessary skills and experience to provide an opinion on the data in question

**Caldicott Guardian (Data Security Standard 1)**
A senior person responsible for protecting the confidentiality of people's health and care information, ensuring it is used correctly and acting as the 'conscience' of the Trust. The Chief Nurse/ Director of Quality & Professions and the Deputy Director of Nursing, Quality & Professions are the Trust's Caldicott Guardians.

**Caldicott Principles**
A set of principles defined by the NDG against which every flow of patient-identifiable data should be justified and routinely tested.

**Competent authority, disclosure to for the prevention or detection of unlawful acts (Data Protection Act 2021 schedule 7)**

- A UK government department other than a non-ministerial department
- Chief officers of police and other police bodies
- Other authorities with investigatory functions
- Authorities with functions relating to offender management
- Other authorities:
    - The Director of Public Prosecution
    - The Director of Service Prosecutions
    - The ICO
    - A court or tribunal

**Consent (UK GDPR article 4.11)**
Any freely given, specific, informed and unambiguous indication of a data subject's wishes that signifies agreement to the processing of personal data about him/ her; N.B. under the EU and UK GDPRs implied consent is unlawful

**Criminal convictions and offences, personal data about**
Personal data about criminal convictions and offences includes, but is not limited to, information about:

- Criminal activity,
- Allegations,
- Investigations,
- Proceedings.
- Unproven allegations,
- Information relating to the absence of convictions,
- Personal data of victims and witnesses of crime,
- Personal data about penalties,
- Conditions or restrictions placed on an individual as part of the criminal justice process, and,
- Civil measures that may lead to a criminal penalty if not adhered to.

**Data Controller (UK GDPR article 4.7)**
A natural or legal person, public authority, agency or other body which, alone or jointly, determines the purpose and means of processing personal data.

**Data Processor (UK GDPR article 4.8)**
A natural or legal person, public authority, agency or other body that processes personal data on behalf of a data controller.
N.B. the means and processing of the personal data are determined by the data controller: the data processor acts on the data controller's instruction

**Data Protection Act 2018**
The law that implemented the EU GDPR into UK law until 31 December 2020; since 1 January 2021 it forms part of the UK's general data protection regime alongside the UK GDPR, making provision for processing personal data that is outside scope of the UK GDPR and providing exemptions from the UK GDPR.

**Data Protection Impact Assessment (DPIA) (Data Security Standard 1)**
A process for analysing, identifying and minimising the data protection risks of a project or plan.

**Data Protection Officer (DPO) (Data Security Standard 1)**
Under UK GDPR article 37 public authorities must designate a DPO to provide information and advice to the data controller, monitor compliance with the UK GDPR, provide advice on DPIAs and act as the contact point with the ICO. The Information Governance Manager is the Trust's DPO.

**Data Security and Protection Standards for Health and Social Care**
Data security standards recommended by the NDG to meet statutory obligations on data protection and data security: compliance is measured through the DSPT.

**Data Security and Protection Toolkit (DSPT)**
An annual self-assessment tool that allows organisations to measure their performance against the NDG's data security and protection standards for health and social care

**Data Subject**
An individual who is identified or identifiable in a record or other information

**Digital Task and Action Group (TAG)**
A Trust group chaired by the Assistant Director of IT Services and Systems Development and attended by the DPO and IAAs, to ensure there is appropriate evidence, assurance and governance regarding digital assets, processes and resources.

**EU General Data Protection Regulation (EU GDPR)**
A regulation in European Union (EU) law on data protection in the EU and European Economic Area (EEA). It was implemented into UK law by the Data Protection Act 2018 and continued to apply after the UK's exit from the EU until 31 December 2020

**Health, data concerning (UK GDPR article 4.15)**
Personal data related to the physical or mental health of a natural person, including the provision of health care services that reveal information about his/ her health status.

**Information Security Lead**
A person responsible for overseeing the management of data controls and providing security assurance for the development and maintenance of information systems. The Head of IT Services & Systems Development is the Trust's information security lead.

**Improving Clinical Information Group (ICIG)**
A Trust group chaired by the Caldicott Guardian and attended by the SIRO, DPO and operational representatives, to ensure there is a robust approach to ensuring high quality clinical information and good information governance.

**Information Asset**
Any electronic or manual system that holds personal, confidential data.

**Information Asset Administrator (IAA)**
An individual, or one of a number of individuals, who use an information asset on a daily basis and are more familiar than the IAO with the information held, the operation of the asset and the risks.

**Information Asset Owner (IAO)**
A senior member of staff who is the nominated owner of one or more information asset.

**Information Commissioner's Office (ICO)**
The UK's supervisory authority responsible for compliance with the UK GDPR and Data Protection Act 2018 and for improving organisations' data protection practices by dealing with concerns raised by the public.

**ISO27001**
An international standard on how to manage information security.

**IT infrastructure**
A combined set of hardware, software, networks and equipment used to develop, test, deliver, monitor, control and support IT services.

**Medical examiner**
A senior medical doctor contracted to provide independent scrutiny of the causes of non-coronial death, outside their usual clinical duties, who has a right of access to health records of the deceased under the provisions of the Access to Health Records Act 1990.

**National Data Guardian (NDG)**
A government appointed individual who advises and challenges the health and care system and advises on how confidential information can be used properly to support care and deliver better outcomes.

**Necessary, processing of personal data must be**
Processing of personal data must be necessary to achieve a specific objective that cannot be achieved using anonymous data or without processing the personal data.

**Personal Data (UK GDPR article 4.1)**
Any information relating to an identified or identifiable natural person (data subject)

**Personal Data Breach (UK GDPR article 4.12)**
A breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure of or access to personal data.

**Personal representative, a deceased person's**
A person who is responsible for settling the affairs of a deceased person, includes both executors and administrators

**Processing (UK GDPR article 4.2)**
Any operation performed on personal data including collection, recording, organisation, storage, alteration, retrieval, consultation, disclosure, dissemination, combination, restriction, erasure or destruction.

**Pseudonymisation (UK GDPR article 4.5)**

The processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is held separately and is subject to technical and organisational measures to ensure the personal data cannot be attributed to an identified or identifiable person

**Removable media**
Portable storage devices that are not permanently attached to computer hardware, including USB/ memory sticks, pen drives, external hard drives, disks, digital cameras, smart phones and audio devices.

**Senior Information Risk Owner (SIRO) (Data Security Standard 1)**
An executive director or other senior member of the board who understands how the strategic business goals of the organisation may be impacted by information risks. The Director of Finance & Resources is the Trust's SIRO.

**Serious crime**
For the purposes of sharing patient data to prevent or detect crime or to apprehend or prosecute offenders without the consent of the data subject, serious crime involves the physical or psychological harm of individuals, including murder, manslaughter, rape, child abuse and neglect.

**Third party**
For the purposes of the security and protection of data concerning health, a third party is any other individual besides:

- The data subject
- A health professional who has been involved in the care of the data subject.
- A health professional or associated staff member who has compiled or contributed to a health record

**UK General Data Protection Regulation (UK GDPR)**
The EU GDPR was amended by the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulation 2019 and the revision is known as the UK GDPR. The UK GDPR became effective on 1 January 2021 and forms part of the UK's general data protection regime alongside the Data Protection Act 2018; it applies to most organisations, setting out data protection principles, rights and obligations.

# 4. Duties

## Accounting Officer

The Chief Executive is the Accounting Officer with responsibility for data security and protection in the Trust and providing assurance through the Trust's Statement of Internal Controls that all risks to the Trust, including those related to information, are effectively managed and mitigated.

## Director Leads

- Providing direction in the formulation, implementation and promotion of compliance with this policy
- Ensuring resources are available to support this policy.
- Being accountable for confidentiality, data security and protection to the EMT, ensuring they are briefed and effectively supported, including advising on issues affecting service delivery.
- Ensuring there is appropriate access to expertise in all aspects of data security and protection.
- Ensuring staff training needs are adequately addressed.
- Developing a culture of data security and protection and information risk awareness
- Establishing working groups as required to coordinate the activities of staff given data security and protection responsibilities.
- Progressing initiatives, ensuring annual assessments and audits of data security and protection policies are undertaken, documented and reported.
- Monitoring data security and protection activities to ensure compliance with guidance and legal requirements.
- Liaising with committees, working groups and programme boards to promote and integrate data security and protection.
- Ensuring the annual assessment and improvement plans are prepared for approval by the EMT.
- Reviewing the relevant risk registers with ICIG and Digital TAG and ensuring actions are reviewed and agreed and reported to the EMT.
- Ensuring the Trust's approach to data security and protection is communicated to all staff and available to the public.

## Senior information Risk Owner (SIRO)

- Leading on information risk management and taking ownership of the risk assessment process
- Understanding how information risks impact the Trust's strategic business goals.
- Advising EMT on information risk issues
- Ensuring the Trust's approach to information security risk is effective in terms of resource, commitment and execution.
- Acting as an escalation point for discussion and resolution of identified risks
- Ensuring personal data breaches are managed.
- Authorising the reporting of serious personal data breaches
- Ensuring critical information assets have appropriate business continuity and disaster recovery plans.
- Ensuring the Audit Committee are updated on risk assessments and outcomes.

## Caldicott Guardian

- Ensuring patient and service user identifiable information is used, transferred and shared appropriately and securely.
- Acting as the “conscience” of the Trust, providing advice on options for the lawful and ethical processing of service user identifiable information
- Providing advice on service user confidentiality, particularly in the context of service development affecting confidentiality
- Making final decisions on proposed breaches of service user confidentiality within the framework of this policy
- Attending working groups as appropriate to ensure the interests of service users are protected.
- Ensuring data security is considered when applications are developed or enhanced.

## Information Governance Manager

- Developing this policy
- Providing advice to all staff on the application and use of this policy
- Supporting and advising the SIRO and Caldicott Guardian
- Ensuring assessments of compliance with the requirements of the DSPT are undertaken regularly and improvement plans are created and approved.
- Managing the DSPT process and ensuring the Trust’s annual submission is completed.
- Managing the information risk register
- Ensuring new information security risks are reported to the SIRO.
- Reviewing incidents and providing appropriate advice and guidance to managers and staff
- Managing the process for mandatory data security and protection training
- Managing the process for recording and approving data flows

## Data Protection Officer

- Monitoring and taking a risk-based approach to organisational compliance with the data protection principles
- Providing regular compliance reports to the SIRO
- Providing advice on compliance to Trust staff
- Providing training and raising awareness
- Providing advice on data protection impact assessments
- Acting as the Trust’s main contact point with the ICO
- Maintaining an expert knowledge of data protection
- Monitoring personal data breaches and recommending appropriate action
- Where appropriate, liaising with Data Protection Officers from partner organisations.
- Reporting personal data breaches to external bodies as required
- To provide advice as regards the DPIA and monitor its performance

### Information Security Lead

- Informing, advising and implementing the Trust's security framework, including the effectiveness of security controls
- Monitoring compliance with a range of legislation and standards, including the security elements of current data protection legislation, ISO27001 and the DSPT
- Responding to and coordinating efforts in relation to security incidents
- Cooperating with the ICO
- Being a champion and advocate for good information security practice in the Trust

### Information Asset Owners (IAOs)

- Ensuring users are aware of and comply with standards of data security and protection and information risk management.
- Identifying and documenting all the information assets that they own and ensuring records of information held are accurate and kept up to date.
- Providing assurance to the SIRO that information risks are managed effectively for the information assets for which they are responsible.
- Supporting the SIRO in maintaining awareness of risks to information assets
- ensuring the system specific security plan (SSSP) risk screening template is completed and sent to the Digital TAG for approval on an annual basis

### Project/ Change Managers

- Ensuring changes to the way Trust information is processed are reviewed and data protection by design requirements are met.
- Ensuring effective security countermeasures are produced and implemented as part of any new systems project
- Ensuring all relevant system documentation relating to operating procedures and disaster recovery/business continuity plans, which reference this policy, are in place as part of the project
- Ensuring all information systems are approved by the service supplier on behalf of, and in conjunction with the Trust, before they commence operation, and that approval is appropriately documented

### Managers

- Ensuring local induction for new starters incorporates data security and protection.
- Ensuring staff are briefed on data security and protection initiatives and policy requirements.
- Enabling policy implementation locally
- Encouraging the reporting of personal data breaches
- Identifying and managing information risks locally
- Ensuring the mandatory data security and protection training target is achieved.
- Nominating and supporting appropriate representatives to attend data security and protection working groups as required.
- Ensuring staff roles are segregated so no individual can carry out and approve process or system changes.
- Ensuring the security of the Trust's information assets

### All Staff

- Completing mandatory data security and protection training on an annual basis as a minimum
- Complying with this policy
- Understanding that failure to comply with this policy may result in disciplinary action.
- Being aware of data security and protection initiatives and policy requirements
- Reporting personal data breaches
- Being aware of information risks and following guidance on how to mitigate them.
- Safeguarding hardware, software and information in their care
- Ensuring information is not permanently saved on the hard drive of Trust desktop computers or laptops or on mobile devices, such as USB sticks
- Preventing the introduction of malicious software on the Trust's systems
- Reporting suspected or actual personal data breaches and near misses
- Meet the standards set out in the Confidentiality: NHS Code of Practice

### Information System Suppliers

- Ensuring systems do not pose an unacceptable security risk to the Trust
- Undertaking checks on or assessments of a system implementation based on any changes made
- Ensuring all connections to external systems are documented and approved
- Ensuring operational systems are monitored for potential security breaches
- Ensuring there is effective configuration management for all systems
- Ensuring systems are regularly checked for compliance with security standards
- Ensuring disaster recovery plans are produced, reviewed and tested
- Ensuring that, where appropriate, Trust IT Services and Systems Development staff receive security awareness training
- Implementing an effective framework for the management of information security in line with the DSPT
- Assisting in the formulation of this policy and related policies and procedures
- Advising on the content and implementation of the relevant action plans
- Producing organisational standards, procedures and guidance on information security matters for approval by the ICIG
- Co-ordinating information security activities, particularly those related to shared information systems or IT infrastructures
- Liaising with external organisations on information security matters, including representing the Trust on cross-community committees
- Creating, maintaining, giving guidance on and overseeing the implementation of guidance relating to information security
- Providing advice and guidance on:
    - Policy compliance
    - Incident investigation
    - IT security awareness
    - Department of Health & Social Care guidance
- Advising users on potential breaches of the UK GDPR or Data Protection Act 2018 and recommending actions

- Promoting awareness of and providing guidance and advice on other legislation and regulations relevant to information security as they apply to the Trust

# 5. Principles

## 5.1. Responsibility of the Trust (UK GDPR article 24)

The Trust shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the UK GDPR.

The Trust shall adhere to approved codes of conduct drawn up by the ICO that are intended to contribute to the proper application of the UK GDPR (article 40).

The Trust shall also adhere to codes of conduct prepared by associations and bodies representing the health and social care sector for the purpose of specifying the application of the UK GDPR (article 40).

### 5.1.1. Audit

The Trust shall comply with any compulsory or consensual audit of its data security and protection practices by internal audit, the ICO, the Department of Health & Social Care and any other audit body as required.

### 5.1.2. Data protection by design and by default (UK GDPR article 25)

At the time that the means of processing personal data are determined and at the time of the processing itself, the Trust shall implement appropriate technical and organisational measures that are designed to implement the principles relating to the processing of personal data (section 5.2 of this policy), in an effective manner, to integrate the necessary safeguards into the processing to meet the requirements of the UK GDPR and to protect the rights of data subjects.

#### 5.1.2.1. Risk assessments

The Trust shall ensure its system specific security policies are reviewed at least annually by the Digital TAG to determine if appropriate and effective information security controls are in place.

### 5.1.3. Responsibility of the data controller (UK GDPR article 26)

The Trust, as a data controller, will determine the purposes and means of processing personal data.

Where the Trust jointly determines the purposes and means of processing personal data with one or more other data controllers, they shall be joint controllers. Data subjects may exercise their rights under the UK GDPR (see section 5.8 of this policy) in respect of and against each of the controllers.

### 5.1.4. Responsibility of the data processor (UK GDPR article 28)

Where processing is to be carried out on behalf of the Trust, the Trust shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the UK GDPR and ensure the protection of the rights of the data subject.

Data processors shall not engage sub-processors without the prior specific or general written authorisation of the Trust.

Processing by a data processor shall be governed by a contract that is binding on the processor with regard to the Trust and that sets out the subject-matter, duration, nature and purpose of the processing, type of personal data, categories of data subject and the obligations and rights of the Trust.

### 5.1.5. Records of processing activities (UK GDPR article 30): information asset registers and data flows

The Trust shall maintain a register of information assets under its responsibility; where the Trust is processing data on behalf of another data controller, a record of all categories of processing activities shall also be maintained.

For the purpose of this policy information sharing is defined as:

- Sharing of personal data between the Trust and one or more third parties outside the Trust, or,
- Sharing information between different parts of the Trust for different or unrelated purposes

All new data flows will be documented and notified to the Digital TAG. All data sharing will be approved by the Caldicott Guardian.

The Trust will not share information outside the UK or a country in the European Economic Area unless explicit approval is obtained from the EMT.

#### 5.1.5.1. Electronic information assets

The Trust shall ensure documented procedures are developed for the operation of new or enhanced systems, based on the analysis of risks; new and amended procedures shall be submitted to the Digital TAG for review and approval.

The Trust shall ensure non-standard software has been approved by the service supplier on behalf of and in conjunction with the Trust prior to installation on Trust equipment; the IAO must ensure software used on Trust equipment has a valid licence agreement.

On behalf of and in conjunction with the Trust, service suppliers shall ensure that mobile computing equipment recommendations meet the Department of Health & Social Care guidelines as a minimum.

#### 5.1.5.2. Electronic data transfers

The Trust shall not extract and transfer personal data by portable removable media, file transfer protocols or email without prior, written approval from the Information Governance Manager.

#### 5.1.5.4. Removable media

The Trust shall only allow authorised staff to use encrypted, removable devices for the purpose of their job role and under the supervision of line management.

#### 5.1.5.5. Third party access to network accounts

The Trust shall permit access to a staff member's account in exceptional circumstances, including to provide cover for long term sick leave.

#### 5.1.6. Cooperation with the ICO (UK GDPR article 31)

The Trust shall cooperate, on request, with the ICO in the performance of the ICO's tasks.

### 5.2. Principles relating to processing of personal data (UK GDPR article 5)

All personal data held by the Trust shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**')

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**')

3. Adequate, relevant and limited to what is necessary in relation to the purpose(s) for which it is processed ('**data minimisation**')

4. Accurate and, where necessary, kept up to date ('**accuracy**')

5. Kept in a form that permits identification of the data subject(s) for no longer than is necessary for the purpose for which it is processed ('**storage limitation**')

   The Trust will retain personal data in line with the retention schedules set out in the Records Management Code of Practice for Health and Social Care 2021

6. Processed in a manner that ensures appropriate security, including protection against unlawful or unauthorised processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**')

### 5.3. Lawfulness of processing (UK GDPR article 6)

The Trust shall ensure processing of personal data it holds is lawful and at least one of the following applies:

1. The data subject has given explicit consent to the processing of his/ her personal data for one or more specific purposes ('**consent**')

   The Trust shall be able to demonstrate that the data subject has consented to processing of his/ her personal data and the data subject shall have the right to withdraw his/ her consent at any time (UK GDPR article 7)

2. Processing is necessary for the performance of a contract to which the Trust is party or in order to take steps at the request of a data subject prior to entering into a contract ('**contract**')

3. Processing is necessary for compliance with a legal obligation to which the Trust is subject ('**legal obligation**')

4. Processing is necessary in order to protect the vital interests of the data subject or another living individual ('**vital interests**')

5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust ('**public task**')

   Under section 8(d) of the Data Protection Act 2018, processing of personal data that is necessary for the performance of a task carried out in the public interest includes processing of personal data that is necessary for the exercise of a function of a government department.

   The Trust shall ensure the public interest in processing its personal data outweighs issues of privacy in situations where consent cannot be obtained and adheres to the Confidentiality: NHS Code of Practice Supplementary Guidance on Public Interest Disclosures.

6. Processing is necessary for the purposes of the legitimate interests pursued by the Trust or a third party ('**legitimate interests**')

   The ICO advise that public authorities can only rely on legitimate interests if the processing is for a legitimate purpose other than performing their tasks as a public authority

## 5.4. Processing of special categories of personal data (UK GDPR article 9)

Processing of data revealing the following is prohibited:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership

Processing of the following data is prohibited:

- Genetic data
- Biometric data
- Data concerning health
- Data concerning person's sexual orientation
- Data concerning a person's sex life
  N.B. data describing the risk of sexual exploitation does not constitute data concerning a person's sex life (Court of Appeal M v Chief Constable of Sussex Police [2021] EWCA Civ 42)

The Trust shall process data listed above if one of the following applies:

1. **Explicit consent**

The data subject has given explicit consent to the processing of the personal data for one or more specified purposes, except where another UK law provides that the prohibition on processing cannot be lifted by the data subject.

Consent is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

2. **Employment, social security and social protection**
   Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the Trust or a data subject in the field of employment and social security and social protection law, in so far as it is authorised under schedule 1, part 1 of the Data Protection Act 2018

   The Data Protection Act 2018 condition is met if the processing is necessary for the purposes of performing or exercising obligations or rights that are imposed or conferred by law on the Trust or a data subject in connection with employment, social security or social protection. The Trust's appropriate policy document for this processing is included in appendix 12.1.

   Employment, social security and social protection is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

3. **Vital interests**
   Processing is necessary to protect the vital interests of the data subject or another living individual where the data subject is physically or legally incapable of giving consent.

   Vital interests are also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

4. **Not-for-profit bodies**
   Processing is carried out in the course of the legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to member or former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subject.

   Not-for-profit bodies is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

5. **Made public by the data subject**
   Processing relates to personal data that is manifestly made public by the data subject.

   Manifestly made public by the data subject is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

6. **Legal claims or judicial acts**

Processing is necessary for the establishment, exercise of defence of legal claims or whenever courts are acting in the judicial capacity.

Legal claims or judicial acts is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

**7. Reasons of substantial public interest**

Processing is necessary for reasons of substantial public interest on the basis of schedule 1 of the Data Protection Act 2018, which shall be proportionate to the aim pursued, respect the right to the essence of data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject. The Trust's appropriate policy document for this processing is included in appendix 12.2.

The following substantial public interest conditions are available under schedule 1 of the Data Protection Act 2018:

- Statutory and government purposes, including the exercise of a function of a government department; statutory and government purposes is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Administration of justice; administration of justice is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Equality of opportunity or treatment, including identifying and keeping under review the existence or absence of equality of opportunity or treatment between groups of people

- Racial and ethnic diversity at senior levels of organisations, where processing is carried out as part of a process of identifying individuals to hold senior positions in an organisation or for the purposes of promoting or maintaining diversity of individuals who hold senior positions

- Preventing or detecting unlawful acts, where the processing must be carried out without the consent of the data subject so as not to prejudice the purpose and disclosure is to a competent authority; preventing or detecting unlawful acts is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Protecting the public against dishonesty, where the processing must be carried out without the consent of the data subject so as not to prejudice the exercise of a protective function, including:
  - Dishonesty, malpractice or seriously improper misconduct,
  - Unfitness or incompetence,
  - Mismanagement in the administration of a body or association, or,
  - Failures in service provided by a body or association.

  Protecting the public against dishonesty is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Regulatory requirements relating to unlawful acts and dishonesty, where processing is necessary to comply with a regulatory requirement that involves a person taking steps to establish where another person has:
  - Committed an unlawful act, including a failure to act, or
  - Been involved in dishonesty, malpractice or other seriously improper conduct.

  and, in the circumstances, the Trust cannot reasonably be expected to obtain the consent of the data subject. Regulatory requirements include:
  - A requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or
  - A requirement forming part of generally accepted principles of good practice relating to a type of body or activity

  Regulatory requirements relating to unlawful acts and dishonesty is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Journalism in connection with unlawful acts and dishonesty, where the Trust reasonably believes that publication of personal data would be in the public interest and the processing is carried out in connection with one of more of the following matters:
  - The commission of an unlawful act be a person,
  - Dishonesty, malpractice or seriously improper conduct of a person,
  - Unfitness or incompetence of a person,
  - Mismanagement in the administration of a body or association,
  - A failure in service provided by a body or association

  Journalism in connection with unlawful acts and dishonesty is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Preventing fraud, where the processing of personal data is:
  - A disclosure made by a person as a member of an anti-fraud organisation,
  - A disclosure made in accordance with arrangements made by an anti-fraud organisation, or,
  - The processing of personal data disclosed as above

  Preventing fraud is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Confidential counselling, advice or support or another, similar service provided confidentially, where the processing is carried out without the consent of the data subject for one of the following reasons:
  - In the circumstances, consent cannot be given by the data subject,
  - In the circumstances, the Trust cannot reasonably be expected to obtain the consent of the data subject,
  - Obtaining the consent of the data subject would prejudice the provision of confidential counselling, advice or support or another, similar service provided confidentially

  Counselling is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

- Safeguarding of children and individuals at risk, where the processing is necessary for the purposes of:
  - Protecting an individual from neglect or physical, mental or emotional harm, or
  - Protecting the physical, mental or emotional wellbeing of a particular individual or a particular type of individual.

  and the individual is:
  - Aged under 18, or,
  - Aged 18 or over and at risk.

  and the processing is carried out without the consent of the data subject for one of the following reasons:
  - In the circumstances, consent cannot be given by the data subject,
  - In the circumstances, the Trust cannot reasonably be expected to obtain the consent of the data subject,
  - Obtaining the consent of the data subject would prejudice the provision of the protection set out above

  For the purposes of processing personal data to safeguard individuals at risk, an individual aged 18 or over is 'at risk' if the Trust has reasonable cause to suspect that the individual:
  - Has needs for care and support,
  - Is experiencing, or at risk of, neglect or physical, mental or emotional harm, and,
  - Is unable to protect him or herself against the neglect or harm or the risk of it

  Safeguarding of children and individuals at risk is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

  The Trust will have regard to the Information Sharing and Suicide Prevention Consensus Statement when deciding whether to share information about an individual's suicide risk.

- Safeguarding of economic wellbeing of certain individuals, where the data subject is aged 18 or over and the processing is of data concerning health is carried out without the data subject's consent for one of the following reasons:
  - In the circumstances, consent cannot be given by the data subject,
  - In the circumstances, the Trust cannot reasonably be expected to obtain the consent of the data subject,
  - Obtaining the consent of the data subject would prejudice the provision of protection

  For the purposes of safeguarding of economic wellbeing, an 'individual at economic risk' is an individual less able to protect his or her economic wellbeing by reason of physical or mental injury, illness or disability

- Occupational pensions, where the processing:
  - Is for the purpose of deciding in connection with eligibility for, or benefits payable under, an occupational pension scheme, as defined in section 1 of the Pension Schemes Act 1993,

- If of data concerning health that relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme,
- Is not carried out for the purposes of measures or decisions with respect to the data subject, and,
- Can reasonably be carried out without the consent of the data subject

Processing can reasonably be carried out without the consent of the data subject only where:

- The Trust cannot reasonably be expected to obtain the consent of the data subject, and,
- The Trust is not aware of the data subject withholding consent, which does not include a data subject failing to respond to a request for consent

- Disclosure to elected representatives, where processing consists of the disclosure of personal data:
  - To an elected representative or a person acting in the authority of such of representative, and,
  - In response to a communication to the Trust from that representative or a person acting in the authority of such of representative.

  and:
  - Personal data is relevant to the subject matter of the communication, and,
  - The disclosure is necessary for the purpose of responding to the communication.

  without the consent of the data subject to one of the following reasons:
  - In the circumstances, consent cannot be given by the data subject,
  - In the circumstances, the elected representative cannot reasonably be expected to obtain the consent of the data subject,
  - Obtaining the consent of the data subject would prejudice the action taken by the elected representative,
  - The processing is necessary in the interests of another individual and that data subject has withheld consent unreasonably

  Disclosure to elected representatives is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

**8. Health or social care**

Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems on the basis of schedule 1 of the Data Protection Act 2018 or pursuant to contract with a health professional and subject to certain additional conditions and safeguards set out in article 9(3) of the UK GDPR.

Schedule 1 of the Data Protection Act 2018 requires that the processing is necessary for health or social care purposes, where ‘health and social care purposes’ means:

- preventative or occupational medicine,
- the assessment of the working capacity of the employee,
- medical diagnosis,
- the provision of health care or treatment,

- the provision of social care, or,
- the management of health care systems or services or social care systems or services.

Article 9(3) of the UK GDPR requires that personal data processed for health or social care purposes is processed by or under the responsibility of a professional subject to the obligation of:

- professional secrecy under the Data Protection Act 2018, or,
- rules established by national, competent bodies, or,
- rules established by another person also subject to an obligation of secrecy under the Data Protection Act 2018 or rules established by national, competent bodies.

Health or social care is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

**9. Public health**

Processing is necessary for reasons of public interest in public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of schedule 1 of the Data Protection Act 2018, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject.

Schedule 1 of the Data Protection Act 2018 requires that processing of personal data for reasons of public interest in public health is carried out by:

- By or under the responsibility of a health professional, or,
- By another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

Public health is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

**10. Archiving, research and statistics**

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) of the UK GDPR, supplemented by section 19 of the Data Protection Act 2018; based on schedule 1 of the Data Protection Act 2018, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

Schedule 1 of the Data Protection Act 2018 requires that processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is:

- Is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- Is carried out in accordance with article 89(1) of the UK GDPR (supplemented by section 19 of the Data Protection Act 2018), and

- Is in the public interest

Article 89(1) of the UK GDPR requires that processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with the UK GDPR, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular to ensure respect for the principle of data minimisation (section 5.1 of this policy). Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing that does not permit of no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Under section 19 of the Data Protection Act 2018, processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes does not satisfy the requirement under article 89(1) of the UK GDPR if:

- it is likely to cause substantial damage or distress to a data subject, or,
- it is carried out for the purposes of measures of decisions with respect to a particular data subject unless the purposes for which the processing is necessary include approved medical research.

Research is also a condition for processing criminal offence and convictions data (section 5.5 of this policy).

## 5.5. Processing of personal data relating to criminal convictions and offences (schedule 1 of the Data Protection Act 2018)

The UK GDPR sets out that this type of data merits specific protection because its use could create significant risks to the individual's rights and freedoms and must be treated differently to other special categories of data.

The Trust does not have official authority to process personal data about criminal convictions and offences.

The Trust shall process personal data relating to criminal convictions and offences where:

- a lawful basis under section 6 of the UK GDPR can be identified (section 5.3 of this policy), and,
- a condition for processing under schedule 1 of the Data Protection Act 2018 can be identified (section 5.4 of this policy).

## 5.6. Duty of Confidentiality

The Trust acknowledges that a duty of confidentiality arises when information is obtained in circumstances where it is reasonable for the person confiding the information to expect that it will be held in confidence by the recipient, which extends beyond death, and is distinct from its obligations under the UK GDPR and DPA 2018.

The Trust acknowledges that, if an individual lacks the competence to expect confided information to be held in confidence, it does not diminish the duty of confidentiality.

The Trust shall engage the Caldicott Guardian and adhere to the Confidentiality – NHS Code of Practice for confidentiality decisions for healthcare purposes, medical purposes other than healthcare and non-healthcare purposes.

#### 5.6.1. Statutory provisions

The Trust shall adhere to the range of statutory provisions that limit or prohibit the use of confidential information in specific circumstances or require confidential information to be used or disclosed for certain purpose.

### 5.7. Caldicott principles

In addition to the UK GDPR principles relating to processing personal data (see section 5.2 of this policy), the Trust shall apply the Caldicott principles to the use of confidential information within the health and social care sector, when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private.

Where a novel and/or difficult judgment or decision is required, the Trust will involve the Caldicott Guardian.

- Principle 1: justify the purpose(s) for using confidential information
- The Trust shall ensure every proposed use or transfer of confidential information is clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian (IAO).
- Principle 2: use confidential information only when it is necessary
- The Trust shall no include confidential information unless it is necessary for the specified purpose(s) for which the information is used or accessed. The Trust shall consider the need to identify individuals at each stage of satisfying the purpose(s) and alternatives used where possible.
- Principle 3: use the minimum necessary confidential information
- Where use of confidential information is necessary, the Trust will justify each item of information so that only the minimum amount of confidential information is included as necessary for a given function.
- Principle 4: access to confidential information should be on a strict need-to-know basis
- The Trust shall ensure only those who need access to confidential information should have access to it, and then only to the items that they need to see.
- Principle 5: everyone with access to confidential information should be aware of their responsibilities
- The Trust shall take action to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

- Principle 6: comply with the law (common law duty of confidentiality)
- The Trust will ensure every use of confidential information is lawful. Trust staff handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.
- Principle 7: the duty to share information for individual care is as important as the duty to protect patient confidentiality
- Trust staff should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of the Trust, regulators and professional bodies
- Principle 8: inform patients and services users how their personal information will be used

The Trust will take a range of steps to ensure no surprises for patients and service users, so they have clear expectations about how and why their confidential information is used and what choices they have.

## 5.8. Rights of the Data Subject

Refer to the Procedure for the Exercise of the Rights of Data Subjects.

### 5.8.1. Transparent information for the exercise of the rights of the data subject (UK GDPR articles 12 and 13)

The Trust shall take appropriate measures to provide the following information to the data subject when personal data is collected:

- The identity and contact details of the Trust,
- The contact details of the DPO,
- The purposes for which the personal data is intended and the legal bases for the processing,
- Where the processing is based on legitimate interests (section 5.2 of this policy), the legitimate interests pursued by the Trust or relevant third party, and,
- The recipients, or categories of recipients, of the personal data, if any.

At the time that personal data is obtained, the Trust will provide the data subject with the following, further information, necessary to ensure fair and transparent processing:

- The period for which the personal data will be stored, or, the criteria used to determine the period,
- The existence of the right to request from the Trust:
    - access to personal data,
    - rectification of personal data,
    - restriction of processing of personal data,
    - cessation of processing of personal data.
- Where the processing is based on consent (sections 5.2 and 5.3 of this policy), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal,
- The right to lodge a complaint with the ICO, and,

- If the provision of personal data is a statutory or contractual requirement (section 5.2 of this policy) and if the data subject is obliged to provide the personal data and the consequences of failure to do so.

Where the Trust intends to further process personal data for a purpose other than for which it was collected, the Trust shall provide the data subject with information on the other purpose prior to the further processing.

**5.8.2. Right of access by the data subject (UK GDPR article 15)**
The data subject shall have the right to obtain from the Trust confirmation as to whether personal data concerning him or her is being processed and, where this is the case, access to the personal data and the following information:

- The purposes of the processing,
- The categories of personal data concerned,
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- The period for which the personal data will be stored, or the criteria used to determine the period,
- The existence of the right to request rectification of personal or restriction of processing of personal data,
- The right to lodge a complaint with the ICO, and,
- Where any personal data was not collected from the data subject, any available as to its source.

**5.8.2.1. Provision of copies of personal data**
At the request of the data subject and subject to the opinion of an appropriate health professional that disclosure will not cause harm to an individual, the Trust shall provide a copy of the personal data being processed on request.

The Trust will not usually charge a fee for processing requests but may charge a reasonable fee based on administrative costs when responding to requests that are manifestly unfounded or excessive.

The Trust may charge a reasonable fee based on administrative costs for requests for further copies of personal data that has already been provided.

The Trust will comply with requests without undue delay and, at the latest, within one calendar month of the date that the request was received, or, if additional information is requested, the data on which sufficient information was received that allowed the request to be processed. The Trust process complex requests within three calendar months.

**5.8.2.2. Health records of the deceased (Access Health Records Act 1990)**
The Trust shall provide information it holds about a deceased person's health only where the requestor can evidence their authority as the deceased's personal representative or provide proof of a claim arising from the death. The Trust shall only disclose information relevant to settling the estate or supporting the claim.

The Trust will make an exception to the duty of confidentiality where records of the deceased are required by statute or a court: the Trust will provide copies of health records of the deceased to the coroner's court and inform of any harm that may arise from releasing the information at the inquest and of any expectations of confidence the deceased had about sharing with family and friends.

On request, the Trust will provide a copy of the health records of a deceased service user to the local medical examiner for independent scrutiny where the death has not been reported to the coroner.

**5.8.2.2.1 Health records of the deceased (NHS England – Transformation Directorate guidance)**
Where a requestor is unable to evidence authority as set out in the Access to Health Records Act 1990 (see section 5.8.2.2 of this policy), the Trust shall provide copies of the personal data to the requestor if, in the opinion of an appropriate health professional, no harm will be caused to an individual. Cases of uncertainty will be referred to the Caldicott Guardian to make recommendations on disclosure.

**5.8.2.3. Personal data held for purposes other than health and employment, social security or social protection**
Data subjects have rights as set out in this section of the policy to all personal and special categories of data that is held by the Trust, other than that held in records that are necessary for health and employment: on receipt of requests for disclosure of such information the Trust will must adhere to the principles of processing personal data (section 5.2 of this policy) and ensure one of the conditions for processing special category (see section 5.4 of this policy) data is met.

**5.8.3. Right to rectification (UK GDPR article 16)**
At the request of the data subject the Trust shall, without undue delay, rectify inaccurate personal data or complete incomplete personal data.

The Trust shall notify any recipients of the personal data that has been rectified unless this proves impossible or involved disproportionate effort. The Trust shall inform the data subject of the recipients if requested. (UK GDPR article 19)

**5.8.4. Right to erasure ('right to be forgotten') (UK GDPR article 17)**
The Trust shall inform data subjects via its privacy materials that the right to be forgotten does not apply where processing of personal data is necessary for reasons of public interest in accordance with health or social care and public health (section 5.3 of this policy) unless the processing is unlawful or must be erased for compliance with a legal obligation.

At the request of the data subject the Trust shall, without undue delay, erase personal data that does not relate to health or social care and public health where one of the following applies:

- the personal data is no longer necessary in relation to the purpose for which it was collected and processed,
- the processing is based on consent and the data subject withdraws consent and there are no other legal grounds for processing,

- the data subject exercises the right to object to the processing (see section 5.8 of this policy) and there are no overriding legitimate grounds for the processing,
- the personal data is being or has been unlawfully processed,
- the personal data must be erased for compliance with a legal obligation.

The Trust will not erase personal data where processing is necessary for one of the following reasons:

- for exercising the right of freedom of expression and information,
- for compliance with a legal obligation
- for the performance of a task carried out in the public interest
- in the exercise of official authority vested in the Trust
- for reasons of public interest in in accordance with health or social care and public health (section 5.4 of this policy)
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (section 5.4 of this policy) insofar as the right to be forgotten is likely to render impossible or seriously impair the achievement of the objectives of that processing
- for the establishment, exercise of defence of legal claims (section 5.4 of this policy)

The Trust shall notify any recipients of the personal data that has been erased unless this proves impossible or involved disproportionate effort. The Trust shall inform the data subject of the recipients if requested. (UK GDPR article 19)

**5.8.5. Right to restriction of processing (UK GDPR article 18)**

The Trust shall restrict processing of personal data where one of the following applies:

- the data subject has contested the accuracy of the personal data: processing will be restricted for a period to enable to the Trust to verify the accuracy,
- the processing is unlawful, and the data subject requests restriction of the data instead of erasure,
- the Trust no longer needs the personal data for the purpose(s) for which it was collected and processed but the data subject needs it for the establishment, exercise or defence of legal claims,
- the data subject has raised an objection to the processing (see section 5.8.7 of this policy): processing will be restricted for a period to enable the Trust to verify the objection and determine whether legitimate grounds override it.

Except for storage, the Trust shall only process restricted personal data with the data subject's consent, for the establishment, exercise of defence of legal claims (section 5.2 of this policy), to protect the rights of another person or for reasons of important public interest.

The Trust shall inform the data subject before the restriction of processing is lifted.

The Trust shall notify any recipients of the personal data that has been restricted unless this proves impossible or involved disproportionate effort. The Trust shall inform the data subject of the recipients if requested. (UK GDPR article 19)

### 5.8.6. Right to data portability (UK GDPR article 20)

The Trust shall inform data subjects via its privacy materials that the right to receive personal data in a structured, commonly used and machine-readable format that can be transmitted to another data controller without hindrance from the Trust does not apply to personal data held on its information assets.

### 5.8.7. Right to object (UK GDPR article 21)

The Trust shall inform data subjects via its privacy materials that there are compelling legitimate grounds for processing of personal data based on its public tasks (paragraph 5, section 5.2 of this policy) that override the interests, rights and freedoms of the data subject; however, the Trust shall not routinely share data concerning health if the data subject does not consent to its processing (section 5.4 of this policy).

The Trust shall no longer process personal data on the basis of its legitimate interests (paragraph 6, section 5.2 of this policy) where a data subject objects to the processing on grounds relating to his or her situation, unless there are compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

### 5.8.8. Automated individual decision-making (UK GDPR article 22)

The Trust shall inform data subjects via its privacy materials that decisions are not based solely on automated processing.

## 5.9. Security of personal data

Refer to the Personal Data Breach Reporting Procedure.

### 5.9.1. NDG's data security standards

The Trust will take the following steps to implement the 10 data security standards across the 3 leadership obligations:

- Leadership obligation 1: people
    - Have a named SIRO, who is a senior executive and a member of the Board, responsible for data and cyber security
    - Complete the DSPT annually, achieving a minimum status of 'standards met'
    - Monitor compliance with the UK GDPR
    - Ensure all staff complete mandatory data security and protection training at least annually

- Leadership obligation 2: process
    - Act on CareCERT advisories on threats to information systems and networks
    - Have comprehensive business continuity plans in place to respond to security incidents, which are documented on the Trust's asset register
    - All Trust staff shall report data security incidents and near misses.

- Leadership obligation 3: technology

- Identify unsupported software and have a plan in place to actively mitigate or manage the associated risks
- Undertake an onsite cyber and data security assessment when invited to do so by NHS Digital
- Check the certification of suppliers of IT systems

**5.9.2. Notification of a personal data breach to the ICO (UK GDPR article 33)**
The Trust shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify a personal data breach to the ICO, unless the nature of the breach is unlikely to result in a risk to the rights and freedoms of any individuals. Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Trust accepts that a personal data breach, or a series of similar breaches, may result in enforcement action being taken by the ICO and shall comply with all requests for information and required actions and have regard to any recommendations.

Lessons learned will be raised at the ICIG or Digital TAG as appropriate.

**5.9.3. Communication of a personal data breach to the data subject (UK GDPR article 34)**
Where a personal data breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust shall communicate it to the data subject without undue delay, adhering to the Trust's Duty of Candour Policy.

**5.9.4. Data protection impact assessment (DPIA) (UK GDPR article 35)**
Where processing is likely to result in a high risk to the rights and freedoms of an individual, the Trust shall, prior to the processing, carry out an assessment of the envisaged processing operations on the protection of personal data.

A DPIA shall be required in the case of processing on a large scale of special categories of data (see section 5.4 of this policy) or of personal data relating to criminal convictions and offences.

The Trust shall seek the advice of the designated DPO when carrying out a DPIA.

**5.9.5. Data protection officer (DPO) (UK GDPR article 37)**
The Trust must designate a DPO, on the basis of professional qualities, expert knowledge of data protection law and practices, and the ability to fulfil the tasks required, as:

- It is a public authority,
- Its core activities consist of processing that requires regular and systematic monitoring of data subjects on a large scale, and
- Its core activities consist of processing on a large scale or special categories of data (see section 5.4 of this policy) or personal data relating to criminal convictions and offences.

#### 5.9.6. DPO position (UK GDPR article 38)

The Trust shall ensure the DPO is involved, properly and in a timely manner, in all issues that relate to the protection of personal data.

The Trust shall support the DPO in performing the required tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain expert knowledge.

The Trust shall ensure the DPO does not receive any instructions regarding the exercise of the required tasks: the DPO shall not be dismissed or penalised by the Trust for performing the required tasks.

The DPO shall directly report to the highest management level of the Trust.

Data subjects may contact the DPO with regard to all issues relating to processing of their personal data and the exercise of their rights under the UK GDPR.

The DPO shall be bound by secrecy and confidentiality concerning the performance of required tasks.

Where the DPO fulfils other tasks and duties, the Trust shall ensure any such tasks and duties do not result in a conflict of interest.

### 5.10. Other Trust Information

#### 5.10.1. Freedom of Information Act 2000

The Trust shall make non-confidential documents and other data available via its publication scheme and on request, in line with its obligations under the Act.

#### 5.10.2. Environmental Information Regulations 2004

The Trust shall make non-confidential environmental information available on request, in line with its obligations under the Regulations.

#### 5.10.3. The Open Government Licence

The Trust shall make its non-confidential publications available for re-use without charge under the licence, ensuring that users acknowledge the Trust as the source of the information and include any attribution statement the Trust may specify.

# 6. POLICY AND STRATEGY
# Equality Impact Assessment template

***This EIA template is to be completed by staff when writing a new policy/strategy or when reviewing a policy/strategy. The EIA needs to demonstrate who would be impacted (local census data and workforce data) and what gaps there are.***

***Any gaps identified need to be included in section 6 where actions are listed to address and progress to ensure inclusivity and diversity in the policy/strategy.***

<table>
<tr><th></th><th>QUESTIONS</th><th>ANSWERS AND ACTIONS</th></tr>
<tr><td>1</td><td>Name of policy/strategy?<br><br>Prompt: is it new or revised?</td><td>Revised Data Security & Protection Policy v1.2</td></tr>
<tr><td>2</td><td>Description of the document:<br><br>Prompt: what is the aim of the document?</td><td>To assure the Executive Management Team (EMT) that the Trust will use and share its personal, confidential data fairly, lawfully and transparently, and will protect the availability, integrity and evidential value and availability of its information, information systems and staff in line with information laws, standards and guidance.</td></tr>
<tr><td>3</td><td>Lead contact person for the Equality Impact Assessment</td><td>Name: Rachael Smith<br><br>Job title: IG Manager</td></tr>
<tr><td>4</td><td>Who else is involved in undertaking this Equality Impact Assessment<br><br>Prompt: list all people involved by name and job title</td><td>Julie Williams, Deputy Director of Corporate Governance</td></tr>
<tr><td>5</td><td>Sources of information used to identify gaps and barriers<br><br>Prompt: local, regional, national research/reports/journals & profession updates. Complaints and compliments data.</td><td><u>Personal data breaches</u><br>Reports to the Improving Clinical Information Group (ICIG) and EMT include gender, ethnicity and age of affected parties; however, age is not a mandatory field in Datix, and the gender and ethnicity fields are often set to ‘unknown’ or ‘not stated’. The author will work with the Nursing & Quality Directorate to improve this.<br><br><u>Workforce data</u><br>There is largely no impact on staff members with protected characteristics as this policy refers to the type of data that is processed, not to the individuals that it is about; however, staff members who have disabilities may have difficulty in understanding or interpreting this policy due to the heavy legislative content and context.<br><br><u>The communities we serve</u><br>This policy is designed for Trust staff use only. Whilst it is acknowledged that members of the public have a right to request copies of policies under the Freedom of Information Act 2000, the Trust’s obligation is to provide a copy of the information that it holds, and there is no requirement to consider barriers to the communities we serve that do not exist for Trust staff.</td></tr>
<tr><td colspan="3">EIA narrative: What does the information you have sourced tell you about the impact your policy/strategy will have on the following equality groups for provision, access and delivery?</td></tr>
<tr><td>5a</td><td>Disability Groups:<br><br>Prompt: consider people who have Learning Disabilities or Difficulties, Physical, Visual, Hearing disabilities and people with long term conditions such as diabetes, cancer, stroke, heart disease. Also consider how you meet their needs in line with the</td><td>
<table>
<tr><th>Area</th><th>Non- disabled</th><th>Disabled</th></tr>
<tr><td>England</td><td>45,715,455<br>82.7%</td><td>9,774,620<br>17.3%</td></tr>
<tr><td>Barnsley</td><td>19,0655<br>78%</td><td>53,920<br>22%</td></tr>
<tr><td>Calderdale</td><td>168,780<br>81.7%</td><td>37,855<br>18.3%</td></tr>
<tr><td>Kirklees</td><td>357,620<br>82.6%</td><td>75,590<br>17.4%</td></tr>
</table>
</td></tr>
</table>

| | | |
|---|---|---|
| | *Accessible information standard.* | |

| | | |
|---|---|---|
| Wakefield | 282,165<br>79.9% | 71,195<br>20.1% |

**Source: Census 2021 data**

**EIA narrative:**
**Managers must be aware that staff with disabilities may have complex needs and must be flexible in recognising and responding appropriately. Alternative formats of this policy will be considered where specific adjustments are required.**

**It should be noted that the Trust's obligation under the UK General Data Protection Regulation to provide access to personal data is to provide a copy of what is held. Therefore, the Trust will not routinely take action to provide copies of personal data in response to requests from staff with disabilities in other formats to that which is held, unless explicit authority is given from a senior manager or above.**

| | **QUESTIONS** | **ANSWERS AND ACTIONS** |
|---|---|---|
| **5 b** | **Gender:**<br><br>*Prompt: Female & Male issues should be considered* | |

| Area | Male | Female |
|---|---|---|
| England | 27,656,336<br>49% | 28,833,712<br>51% |
| Barnsley | 120,279<br>49.2% | 124,293<br>50.8% |
| Calderdale | 100,790<br>48.7% | 105,901<br>51.3% |
| Kirklees | 212,346<br>49% | 220,870<br>51% |
| Wakefield | 173,831<br>49.2% | 179,539<br>50.8% |

**Source: Census 2021 data**

**EIA narrative:**
**No impact on staff using policy.**

**Gender field for affected parties in Datix is usually set to 'unknown' or 'not stated'. Therefore, there is insufficient data to identity inequalities (refer to Action Plan).**

**5c** **Age:**

*Prompt: Older people & Young People issues should be considered*

| Area | Under 18 | 18-39 | 40-59 | 60-79 | Over 80 |
|---|---|---|---|---|---|
| England | 11,774,609<br>20.8% | 16,161,002<br>28.6% | 14,897,132<br>26.4% | 10,858,911<br>19.2% | 2,798,379<br>5% |
| Barnsley | 50,068<br>20.5% | 65,448<br>26.8% | 65,850<br>26.9% | 51,606<br>21.1% | 11,595<br>4.7% |
| Calderdale | 45,122<br>21.8% | 51,990<br>25.2% | 57,280<br>27.7% | 42,548<br>20.6% | 9,694<br>4.7% |
| Kirklees | 98,029<br>22.6% | 11,9116<br>27.5% | 114,735<br>26.5% | 81,845<br>18.9% | 19,484<br>4.5% |
| Wakefield | 73,625<br>20.8% | 96,756<br>27.4% | 94,822<br>26.8% | 71,717<br>20.3% | 16,440<br>4.7% |

**Source: Census 2021 data**

**EIA narrative:**
**No impact of staff using policy.**

**The Date of Birth (DOB) field in Datix is rarely completed. Therefore, there is insufficient data to precisely identity inequalities (refer to Action Plan). Reports to ICIG and EMT show that 21% of personal data breaches reported during the current financial year (April to November) occurred in CAMHS and the Barnsley General Community Services children's teams.**

**5 d** **Sexual Orientation:**

*Prompt: Heterosexual, Bisexual, Gay, Lesbian groups should be considered*

| Area | Straight or heterosexual | Gay or lesbian | Bisexual | Other sexual orientation | Not answered |
|---|---|---|---|---|---|
| England | 43,403,110<br>89.37% | 747,805<br>1.54% | 623,504<br>1.29% | 165,305<br>0.34% | 3,626,649<br>7.46% |
| Barnsley | 182,948<br>91.57% | 2,990<br>1.5% | 1,817<br>0.91% | 396<br>0.2% | 11,638<br>5.83% |
| Calderdale | 149,815 | 2,811 | 1,968 | 550 | 11,488 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 89.91% | 1.69% | 1.18% | 0.33% | 6.89% |
| | Kirklees | 311,501<br>89.96% | 4,340<br>1.25% | 3,697<br>1.07% | 998<br>0.29% | 25,742<br>7.43% |
| | Wakefield | 261,615<br>90.98% | 4,321<br>1.50% | 2,968<br>1.03% | 689<br>0.24% | 17,945<br>6.24% |

**Source: Census 2021 data**

**EIA narrative:**

**No impact**

**5e** **Religion or Belief:**

*Prompt: Main faith groups and people with no belief or philosophical belief issues should be considered*

| Area | Christian | Buddhist | Hindu | Jewish | Muslim | Sikh | Other | No religion | Not answered |
|---|---|---|---|---|---|---|---|---|---|
| England | 26,167,899<br>46.3% | 262,433<br>0.5% | 1,050,533<br>0.5% | 269,283<br>0.5% | 3,801,186<br>6.7% | 420,383<br>0% | 322,410<br>0.6% | 20,715,664<br>36.7% | 3,400,548<br>6.0% |
| Barnsley | 125,502<br>51.3% | 435<br>0.2% | 416<br>0.2% | 62<br>0% | 1,404<br>0.6% | 256<br>0.1% | 862<br>0.4% | 102,906<br>42.1% | 1,2728<br>5.2% |
| Calderdale | 85,677<br>41.5% | 630<br>0.3% | 1,173<br>0.6% | 153<br>0.1% | 19,650<br>9.5% | 387<br>0.2% | 1,045<br>0.5% | 86,787<br>42% | 11,129<br>5.4% |
| Kirklees | 170,577<br>39.4% | 996<br>0.2% | 1,723<br>0.4% | 187<br>0% | 80,046<br>18.5% | 3,476<br>0.8% | 1663<br>0.4% | 150,599<br>34.8% | 23,949<br>5.5% |
| Wakefield | 173,070<br>49% | 797<br>0.2% | 1,270<br>0.4% | 127<br>0% | 11,279<br>3.2% | 501<br>0.1% | 1,405<br>0.4% | 145,950<br>41.3% | 18,972<br>5.4% |

**Source: Census 2021 data**

**EIA narrative:**
**No impact**

**5f** **Marriage and Civil Partnerships**

*Prompt: Single, Married, Co-habiting, Widowed, Civil Partnership status should be considered*

| Area | Married or in a registered civil partnership | Single – never married and never registered in a civil partnership | Divorced | Widowed | Separated |
|---|---|---|---|---|---|
| England | 20,561,642<br>44.7% | 17,450,122<br>37.9% | 4,171,639<br>9.1% | 2,790,036<br>6.1% | 1,033,518<br>2.2% |
| Barnsley | 87,177<br>43.6% | 73,099<br>36.6% | 21,183<br>10.6% | 13,531<br>6.8% | 4,799<br>2.4% |
| Calderdale | 73,651<br>44.2% | 60,324<br>36.2% | 17,611<br>10.6% | 10,794<br>6.5% | 4,254<br>2.6% |
| Kirklees | 159,426<br>46% | 125,290<br>36.2% | 32,022<br>9.2% | 21,509<br>6.2% | 8,027<br>2.3% |
| Wakefield | 127,965<br>44.5% | 103,484<br>36% | 30,105<br>10.5% | 19,017<br>6.6% | 6,966<br>2.4% |

**Source: Census 2021 data**

**EIA narrative:**
**No impact**

**5 g** **Pregnancy and Maternity**

*Prompt: Currently pregnant or have been pregnant in the last 12 months should be considered*

| Area | Number of live births 2021 | Percentage of Total fertility rate (TFR) |
|---|---|---|
| England | 595,948 | 1.55% |
| Barnsley | 2,521 | 1.63% |
| Calderdale | 2,143 | 1.71% |
| Kirklees | 4,826 | 1.72% |
| Wakefield | 3,857 | 1.68% |

**Source: Births in England and Wales: summary tables – Office for National Statistics**

NB: The TFR is the average number of live children that a group of women would bear if they experienced the age-specific fertility rates of the calendar year in question throughout their childbearing lifespan. The national TFRs have been calculated using mid-year population estimates by single year of age. The sub-national TFRs have been calculated using mid-year population estimates by 5-year age group

**EIA narrative:**
**No impact**

**5 h** **Gender Re-assignment**

*Prompt: Transgender issues should be considered*

| Area | Gender identity the same as sex registered at birth | Gender identity different from sex registered at birth | Not answered |
|---|---|---|---|
| England | 43,002,331 | 251,844 | 2,752,783 |

| | | | | |
|---|---|---|---|---|
| | | 93.47% | 0.55% | 5.98% |
| | Barnsley | 189,640<br>94.92% | 803<br>0.74% | 9,389<br>4.70% |
| | Calderdale | 156,893<br>94.16% | 829<br>0.89% | 8,966<br>5.38% |
| | Kirklees | 323,432<br>93.40% | 1,725<br>0.9% | 21,214<br>6.13% |
| | Wakefield | 271,795<br>94.52% | 1,280<br>0.81% | 14,539<br>5.06% |

**Source: Census 2021 data**

*NB: P*ercentages are calculated from the total usual resident population aged 16 years and over

**EIA narrative:**
**No impact**

**5l** **Carers**

*Prompt: Caring responsibilities paid or unpaid should be considered*

| Area | Yes – provide unpaid care | No – do not provide unpaid care |
|---|---|---|
| England | 4,678,265<br>8.3% | 48,734,833<br>86.3% |
| Barnsley | 24,732<br>10.1% | 206,377<br>84.4% |
| Calderdale | 17,977<br>8.7% | 206,631<br>85.8% |
| Kirklees | 37,034<br>8.5% | 371,038<br>85.6% |
| Wakefield | 31,731<br>6.1% | 301,565<br>85.3% |

**Source: Census 2021 data**

*NB: Missing values account for 'N/A' or 'not answered'*

**EIA narrative:**
**No impact**

**5j** **Race**

*Prompt: Indigenous population and BME Groups such as black African and Caribbean, mixed heritage, South Asian, Chinese, Irish, new migrant, asylum & refugee, gypsy & travelling communities)*

| Area | White | Asian | Black | Mixed | Chinese & other |
|---|---|---|---|---|---|
| England | 45,783,401<br>81% | 5,426,392<br>9.6% | 2,381,724<br>4.2% | 1,669,378<br>3% | 1,229,153<br>2.1% |
| Barnsley | 236,964 (96.6%) | 2,297 (0.9%) | 1,715<br>(0.7%) | 2,293<br>(0.9%) | 1,333<br>(0.5%) |
| Calderdale | 177,836<br>(86.1%) | 21,726<br>(10.5%) | 1,439<br>(0.7%) | 4,027<br>(1.9%) | 1,603<br>(0.8%) |
| Kirklees | 318,969<br>(73.6%) | 84,202<br>(19.4%) | 9,948<br>(2.3%) | 13,588<br>(3.1%) | 6,506<br>(1.5%) |
| Wakefield | 328,742<br>(93%) | 12,633<br>(3.6%) | 4,516<br>(1.3%) | 4,938<br>(1.4%) | 2,541<br>(0.7%) |

**Source: Census 2021 data**

**EIA narrative:**
**No impact on staff using policy.**

**Ethnicity field for affected parties in Datix is usually set to 'unknown' or 'not stated'. Therefore, there is insufficient data to identity inequalities (refer to Action Plan).**

**Involvement & Insight:** Please list in the box below any involvement activity, reports or insight you have gathered by working with your staff team or service users/carers by involving them to gain their views on your service.

Improving Clinical Information Group
Digital TAG
Corporate Policies Group

Under-reporting of and lack of function to report protected characteristics on Datix means themes and inequalities cannot currently be identified.

## 6. Action Plan

EIAs are now reviewed using a grading approach which is in line with our Equality Delivery System (EDS). This rates the quality of the EIA. This means that the team can review the EIA and make recommendations only. The rating and suggested standards are set out below:

- **Under-developed** – red – **No data**. **No strands** of equality
- **Developing** – amber – **Some census data plus workforce**. **Two strands** of equality addressed.
- **Achieving** – green – **Some census data plus workforce. Five strands** of equality addressed.
- **Excelling** – purple – **All the data and all the strands** addressed

Potential themes for actions: Geographical location, built environment, timing, costs of the service, make up of your workforce, stereotypes and assumptions, equality monitoring, community relations/cohesion, same sex wards and care, specific issues/barriers.

**Previous actions update: please explain what progress you have made against the previous actions identified**

**1. IG Manager to work with PSST to improve capture of protected characteristics data for affected parties – PSST have sent out communications and include in training**

**2. IG Manager to work with PSST to capture data on protected characteristics not currently available in Datix – PSST aware of issue and work ongoing**

| Who will benefit from this action? (tick all that apply) | | Action 1: This is what we are going to do | Lead/s | By when | Update -outcome | RAG |
|---|---|---|---|---|---|---|
| Age | X | IG Administrator (appointed 30/11/2023) to commence adding protected characteristics from health record to Datix on first review of new incidents so themes | Rachael Smith | 31/01/2024 | | |
| Disability | | | | | | |
| Gender reassignment | | | | | | |
| Marriage and civil partnership | | | | | | |
| Race | X | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Religion or belief** | | and inequalities can be identified | | | | |
| **Sex** | X | | | | | |
| **Sexual Orientation** | | | | | | |
| **Pregnancy maternity** | | | | | | |
| **Carers** | | | | | | |

**7 Please state what methods of monitoring you are using to progress actions**

Reports to ICIG (six-weekly)

**8 Will you publish the Equality Impact Assessment? Please state where the EIA will be shared or published.**

Once it has been finally approved.

**9 EIA assessment by equality and involvement team**

**Name: Aboobaker Bhana**

**Date: February 2027**

**Rating: Developing**

**Recommendations: Policies need reviewing every three years so not sure why this has an annual review date?**

***When you have fully completed all sections of the EIA and it has been signed off in service, you must email a copy to: InvolvingPeople@swyt.nhs.uk for grading***

**Please note that the EIA is a public document and may be published.**

**Failing to complete an EIA every year could expose the Trust to future legal challenge, as it is a legal requirement to write, review and implement in every service as part of meeting the Equality Act.**

## 7. Dissemination and Implementation Arrangements

Once approved, the Corporate Governance Manager will add this policy to the document store on the intranet and include it in the staff brief.

Where copies of this policy are downloaded and printed locally, a staff member must take responsibility for updating the paper version when a policy change is communicated via the staff brief.

The following training is required:

| | | |
|---|---|---|
| All staff | • Legal and statutory duties<br>• Responsibilities under this policy | • Annual, mandatory IG and data security essentials training<br>• Induction and supervision |
| Caldicott Guardian | Confidentiality skills, knowledge and experience | • Caldicott masterclass at least three-yearly<br>• Annual assessment by approved Caldicott Guardian Health & Social Care workbook otherwise |
| Information Asset Owners (IAOs)/ Administrators (IAAs) and other identified staff as required | Requirements for privacy impact assessments and data sharing arrangements | One-off, in-house understanding privacy impacts and data sharing training |
| Information Governance (IG) Lead/ Data Protection Officer | Industry approved qualification in current data protection legislation<br><br>Knowledge sharing and professional development | Approved classroom training delivered by external provider<br><br>Membership of Strategic IG Network regional sub-group |
| Senior Information Risk Owner (SIRO) | Information risk management skills, knowledge and experience | Annual assessment by approved Risk Management for SIROs workbook |

## 8. Process for Monitoring Compliance and Effectiveness

Information governance incident numbers, categories and learning are reported to the ICIG, which reports to the Clinical Governance Committee.

Breaches of confidentiality are reported to the Trust Board via the Integrated Performance Report.

The Information Governance Manager provides a monthly report to EMT, via the SIRO, which includes incident hot spots and actions taken.

A standing agenda item is included at the Digital TAG for attendees (IAOs/ IAAs) to communicate key messages regarding incident hot spots and required actions to their relevant areas.

| | **Standard** | **Monitoring process - evidence:** |
|---|---|---|
| 1. | This document is reviewed and updated in accordance with Trust policy | The document on the intranet is up to date |
| 2. | Relevant staff will be made aware of the policy and offered support and training | • Document is on the intranet<br>• Reference in team brief<br>• Record of meetings where implementation discussed<br>• Content of and attendance at relevant training<br>• Audit of staff awareness |
| 3. | ICIG will use the number of incidents to monitor the effectiveness of the policy | ICIG to monitor incident numbers, categories and teams to report to Clinical Governance and recommend action plans |
| 4. | Digital TAG will use the categories of incidents to monitor the effectiveness of the policy and identify issues and training needs | Digital TAG to monitor incident types to report to ICIG |
| 5. | Review of action plans | ICIG to review recommendations and action plans where appropriate. |

## 9. Review and Revision Arrangements

This policy will be reviewed at least annually.

Revisions will be made if a risk is identified, in response to learning from a personal data breach or in accordance with changes to legislation, standards or other Trust policies that have an impact on this policy.

## 10. References

- Access to Health Records Act 1990
- Confidentiality: NHS Code of Practice
- Confidentiality: NHS Code of Practice Supplementary Guidance on Public Interest Disclosures
- Data Protection Act 2018Data Protection, Privacy & Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- ICO Guide to the UK GDPR
- Information Security Management: NHS Code of Practice
- Information Sharing & Suicide Prevention Consensus Statement

## 11. Associated Documents

The following are available from the Information Governance Manager/ DPO:

Data Sharing & Handling Procedure
Procedure for the Exercise of Data Subjects' Rights
Reporting Personal Data Breach Reporting & Management Procedure

The following is available on the Document Store:

Being Open Policy (Duty of Candour)

## 12. Appendices

### 12.1. Appropriate Policy Document: data processed for the purposes of employment, social security and social protection

**Description of data processed**

- Employees' contact details, financial information, demographic information including protected characteristics, data relating to health, criminal offence data, emergency contacts, pension dependents, training records, information relating to the disciplinary and capability procedure and sickness absence policy
- Applicants' demographic information, protected characteristics, referees
- Emergency contacts' personal data and contact details
- Pension dependents' personal data and contact details
- Referees' personal data and contact details

**Schedule 1 condition for processing**

Part 1, section 1

**Procedure for ensuring compliance with the principles**

Accountability principle

The Trust:

- Maintains an information asset register of processing activities
- Raises awareness of this policy and related procedures
- Carries out DPIAs for new and amended uses of personal data
- Puts written sharing agreements in place with organisations that process the Trust's personal data
- Has implemented and maintains appropriate technical and organisation security measures
- Records personal data breaches and reports them to the ICO where necessary
- Has appointed at DPO
- Adheres to the relevant codes of conduct (as referenced in this policy)

Lawfulness, fairness & transparency

The Trust:

- Has identified a lawful basis for processing personal data about its workforce ('public task')
- Has identified a condition for processing special categories of data and criminal offence data about its workforce ('employment, social security and social protection')
- Has considered how the processing may affect the individuals concerned and can justify any adverse impact
- Only handles confidential data about its workforce in ways it would reasonably expect; the Trust can justify any unexpected processing
- Does not deceive its workforce when collecting personal data
- Is open, honest and transparent and complies with the transparency obligation of the right to be informed

Purpose limitation
The Trust:

- Has clearly identified the purpose(s) for processing personal data about its workforce, and these are document in the asset register
- Has included details of the purposes for processing personal in our privacy materials
- Reviews its processing activities regularly and, where necessary, updates the asset register and privacy materials

Data minimisation
The Trust:

- Only collects personal data that is need for our specified purposes
- Has sufficient personal data to fulfil its specified purposes
- Periodically reviews the data it holds and deletes anything no longer required for the purpose for which it was collected, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)

Accuracy
The Trust:

- Ensures the accuracy of data it creates
- Has appropriate measures in place to check the accuracy of data collected and record the source of that data
- Has a process in place to identify when the data needs to be kept updated to properly fulfil our purposes, and it is updated as necessary
- Records clearly identify matters of opinion and, where appropriate, whose opinion it is and any relevant changes to the underlying facts
- Complies with individuals' right to rectification and carefully considers and keeps a record of any challenges to the accuracy of personal data

Storage limitation
The Trust:

- Knows what personal data it holds and why it is held
- Carefully considers and can justify how long personal data is held for, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)
- Has a Non-clinical Records Management Policy
- Regularly reviews the personal data it holds and erases personal data that is no longer needed for the purpose for which it was collected, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)
- Has appropriate processes in place to comply with individuals' requests for erasure of information held by the Trust for purpose of its legitimate interests under the 'right to be forgotten'
- Identifies any personal data that needs to be kept for public interest archiving, scientific or historical research, or statistical purposes

Integrity & confidentiality
The Trust:

- Undertakes analyses of the risks presented by our processing, and uses them to assess the appropriate level of security we need to put in place
- When deciding what measures to implement, takes account of the state of the art and costs of implementation
- Includes information security in this policy, has a Sharing and Handling Information Procedure and takes steps to make sure they are implemented
- Where necessary, has additional policies and ensures that controls are in place to enforce them
- Ensures that there is a regular review information security policies, procedures and measures and, where necessary, improves them
- Has assessed what we need to do by considering the security outcomes we want to achieve.
- Has put in place basic technical controls, including those specified by Cyber Essentials Plus
- Understands that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process
- Uses encryption and/or pseudonymisation where it is appropriate to do so
- Understands the requirements of confidentiality, integrity and availability for the personal data we process
- Ensures that access to personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process
- Conducts regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement
- Ensures that any data processor we use also implements appropriate technical and organisational measures.

**Retention and erasure policies**
The Trust retains and erases personal data about its workforce in adherence to the Records Management Code of Practice for Health & Social Care 2021.

**Review date**
This document will be reviewed in line with the policy review.

## 12.2. Appropriate Policy Document: processing of special categories of personal data for reasons of substantial public interest

**Description of data processed**
Processing of data revealing the following:
- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership

Processing of the following data:
- Genetic data
- Biometric data
- Data concerning health
- Data concerning a person's sexual orientation
- Data concerning a person's sex life

**Schedule 1 condition for processing**
Part 1:
- section 6 – statutory and government purposes
- section 7 – administration of justice
- section 8 – equality of opportunity or treatment
- section 9 – racial and ethnic diversity at senior levels of the Trust
- section 10 – preventing or detecting unlawful acts
- section 11 – protecting the public against dishonesty
- section 12 – regulatory requirements relating to unlawful acts and dishonesty
- section 13 – journalism in connection with unlawful acts and dishonesty
- section 14 – preventing fraud
- section 17 – confidential counselling
- section 18 – safeguarding of children and individuals at risk
- section 19 – safeguarding of economic wellbeing of certain individuals
- section 21 – occupational pensions
- section 23 – elected representatives responding to requests

**Procedure for ensuring compliance with the principles**

<u>Accountability principle</u>
The Trust:
- Maintains an information asset register of processing activities
- Raises awareness of this policy and related procedures
- Carries out DPIAs for new and amended uses of special categories of personal data
- Puts written sharing agreements in place with organisations that process the Trust's special categories of personal data
- Has implemented and maintains appropriate technical and organisation security measures
- Records personal data breaches and reports them to the ICO where necessary

- Has appointed at DPO
- Adheres to the relevant codes of conduct (as referenced in this policy)

Lawfulness, fairness & transparency

The Trust:

- Has identified a lawful basis for processing personal data ('public task')
- Has identified a condition for processing special categories of data ('substantial public interest')
- Has considered how the processing may affect the individuals concerned and can justify any adverse impact
- Only handles special categories of data in ways it would reasonably expect; the Trust can justify any unexpected processing
- Does not deceive individuals when collecting special categories of personal data
- Is open, honest and transparent and complies with the transparency obligation of the right to be informed

Purpose limitation

The Trust:

- Has clearly identified the purpose(s) for processing special categories of personal data, and these are documented in the asset register
- Has included details of the purposes for processing special categories of personal data in our privacy materials
- Reviews its processing activities regularly and, where necessary, updates the asset register and privacy materials

Data minimisation

The Trust:

- Only collects special categories of personal data that is need for our specified purposes
- Has sufficient special categories of personal data to fulfil its specified purposes
- Periodically reviews the data it holds and deletes anything no longer required for the purpose for which it was collected, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)

Accuracy

The Trust:

- Ensures the accuracy of data it creates
- Has appropriate measures in place to check the accuracy of data collected and record the source of that data
- Has a process in place to identify when the data needs to be kept updated to properly fulfil our purposes, and it is updated as necessary
- Records clearly identify matters of opinion and, where appropriate, whose opinion it is and any relevant changes to the underlying facts
- Complies with individuals' right to rectification and carefully considers and keeps a record of any challenges to the accuracy of special categories of personal data

Storage limitation

The Trust:

- Knows what special categories of personal data it holds and why it is held
- Carefully considers and can justify how long special categories of personal data are held for, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)
- Has a Health Records Management Policy and Non-clinical Records Management Policy
- Regularly reviews the special categories of personal data it holds and erases data that is no longer needed for the purpose for which it was collected, subject to the Records Management Code of Practice for Health & Social Care 2021 (see below)
- Has appropriate processes in place to comply with individuals' requests for erasure of information held by the Trust for purpose of its legitimate interests under the 'right to be forgotten'
- Identifies any special categories of personal data that needs to be kept for public interest archiving, scientific or historical research, or statistical purposes

Integrity & confidentiality

The Trust:

- Undertakes analyses of the risks presented by our processing, and uses them to assess the appropriate level of security we need to put in place
- When deciding what measures to implement, takes account of the state of the art and costs of implementation
- Includes information security in this policy, has a Sharing and Handling Information Procedure and takes steps to make sure they are implemented
- Where necessary, has additional policies and ensures that controls are in place to enforce them
- Ensures that there is a regular review information security policies, procedures and measures and, where necessary, improves them
- Has assessed what we need to do by considering the security outcomes we want to achieve.
- Has put in place basic technical controls, including those specified by Cyber Essentials Plus
- Understands that we may also need to put other technical measures in place depending on our circumstances and the type of special categories of personal data we process
- Uses encryption and/or pseudonymisation where it is appropriate to do so
- Understands the requirements of confidentiality, integrity and availability for the special categories of personal data we process
- Ensures that access to special categories of personal data can be restored in the event of any incidents, such as by establishing an appropriate backup process
- Conducts regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement
- Ensures that any data processor we use also implements appropriate technical and organisational measures.

**Retention and erasure policies**
The Trust retains and erases special categories of personal data in adherence to the Records Management Code of Practice for Health & Social Care 2021.

**Review date**
This document will be reviewed in line with the policy review.

## 13. Version Control

| Version | Date | Author | Status | Comment / changes |
|---|---|---|---|---|
| 1 | August/ September 2021 | Rachael Smith | Final | Lead Serious Investigator: inclusion of suicide consensus statement<br>Barnsley GCS ICIG rep: corrections made, and clarity added around points raised.<br>Equality & Involvement Manager: revision of EIA to include data sets relevant to combining of six former policies.<br>Head of Corporate Governance: numbering/ bullet points aligned to margins, exploration of easy-read version added to EIA, further information added to EMT proforma for approval |
| 1.1 | September/ October 2022 | Rachael Smith | Final | |
| 1.2 | November 2023 | Rachael Smith | Draft | Inclusion of medical examiner's right of access to health records of the deceased for non-coronial deaths and amendments as advised by lead director |