Shropshire Community Health
NHS Trust

Data Protection Policy

Controlled document

This document is uncontrolled when downloaded or printed

**Author(s)
Owner(s)**
	Author: IG Manager
	Owner: Director of Governance

Version No.	Version 1.5
Approval date	June 2023
Review date	June 2026

Document Details	
Title	Data Protection Policy
Trust Ref No	
Local Ref (optional)	
Main points the document covers	Data protection principles, Individuals’ rights, incident reporting, roles and responsibilities.
Who is the document aimed at?	This policy is aimed at all staff
Author Owner	Head of Information Governance Director of Governance Senior Information Risk Owner (SIRO)
Approval process	
Who has been consulted in the development of this policy?	Data Security and Protection Assurance Group
Approved by (Committee/Director)	Audit Committee, chaired by Non-Executive Director
Approval Date	16 June 2023
Initial Equality Impact Screening	May 2018
Full Equality Impact Assessment	
Lead Director	Director of Governance/Senior Information Risk Owner (SIRO)
Category	General
Sub Category	Information Governance
Review date	16 June 2026
Distribution	
Who the policy will be distributed to	The Data Protection Liaison Officers (DPLOs), Information Governance Team, all staff
Method	Websites, email and Trust Newsletter
Keywords	PID; personal; identifiable; data; PII; information; person; confidential; sensitive
Document Links	
Required by CQC	Yes – Well Led
Other	
Amendments History	

No	Date	Amendment
1	January 2022	Data Protection extracted from the IG Policy (now obsolete) and this separate policy created. Author: Gill Richards Version: 0.1 Page: Whole Document
2	July 2022	Page 2 Owner and author amended
3	July 2022	Update to IT Service Manager description
4	July 2022	Data Security and Protection Assurance Framework updated
5	July 2022	Update 12.2 role of DPLO in Individual Rights request
6	October 2022	Update Owner - Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
7	March 2023	Amended IG Manager to Head of IG. Updated the Safe haven statement. Updated IAO role statement, removed list of IAO responsibilities. Updated list of related policies. Amended Risk Manager to Head of Clinical Governance. IG Assurance Framework updated.
8	20 Feb 2024	Updated: IG job titles and contact details.
9	31 May 2024	Included paragraph re the use of Consent as lawful basis.

This copy is uncontrolled unless printed on ‘Controlled’ paper.

CONTENTS

Contents

1 Policy statement

1.1 Shropshire Community Health NHS Trust (hereafter the Trust) is committed to ensuring that all personal data we process, including that of our staff and colleagues, patients and service users, is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as “DP legislation”).

1.2 Patients and staff trust us to take care of their personal data and will build productive relationships with us based on this trust.

1.3 This policy complies with our obligation in DP legislation to have an appropriate policy document in place where we are processing special category personal data for the purpose of employment obligations and substantial public interest reasons (see Article 9 of UK GDPR and Section 10 and Schedule 1 of the DPA 2018)

1.4 Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

2 Related documents

Policies can be found in the Trust’s Document Library on Public Website and Staff Zone

- Information Security Policy
- Information Asset Register
- Records and Document Management Policy
- Information Risk Policy
- National Data Opt-Out Policy
- Registration Authority Policy
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act
- Information Governance Procedures/Standard Operating Procedures

This document includes links to guidance published by the UK Information Commissioner’s Office (ICO) and by the European Data Protection Board (EDPB).

3 Purpose

3.1 This policy describes the plan of action that will be adopted to ensure that Shropshire Community Health NHS Trust meets its legal obligations under the data protection legislation.

4 Scope

4.1 This Policy entails all personal data held by, or on behalf of The Trust, its processing, storage, handling and usage. Such data includes but is not limited to:

- employee and staff records
- patient/client data and records
- personal data relating to volunteers working with the Trust; personal data in all formats including, but not limited to, paper copy, digital records and CCTV

5 Applicability

5.1 All staff that are required to work within the organisation, employed and non-employed, must adhere to this policy and associated policies. Including, but not limited to:

- Employed staff (including Bank staff)
- Volunteers
- Student Placements
- Medical Placements
- Allied Healthcare Placements
- Locums
- Agency
- Temporary and Fixed Term contracts
- Third Party Suppliers

6 Responsibilities

6.1 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Under the data protection legislation, the Trust is required to demonstrate that it has an information governance framework supported by the following roles:

6.2 The **Board** provides leadership on the management of risk and ensures the approach to risk management is consistently applied as well as determining the information risk appetite for the Trust. The Board is also responsible for setting the Trust's Risk Appetite regarding information security.

6.3 The **Senior Information Risk Owner (SIRO)** is the Board's executive level delegate responsible for risk management including oversight of data protection and other aspects of information governance. The role of the SIRO is to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board, including internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control (SIC) with regards to information risk. The SIRO will advise the Chief Executive and the Board on information risk management strategies, provide periodic reports and briefing on risk management assurance and ensure that key risks are appropriately logged on the corporate risk register.

6.4 The **Chief Executive** is the Accountable Officer and has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation. They have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. The organisation will set out a line of accountability, responsibility and direction in accordance with the guidance set out in the Data Security and Protection Toolkit (DSPT) Standard 1 Personal Confidential Data, example diagram given below.

6.5 The **Chief Information Officer (CIO)** is an executive within the organisation that oversees the operation of the information technology department and consults with other personnel on technology-related needs and purchasing decisions. The CIO is the Head of Digital Services.

6.6 The **Caldicott Guardian (CG)** has responsibility for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. For any patient confidentiality issues the first point of contact should be the CG.   The CG is also the designated **Privacy Officer.**

6.7 The **Chief Clinical Information Officer (CCIO)** is an executive within the organisation who is involved in change management, ensuring clinical adoption and engagement in the use of technology, supporting clinical process redesign in a digital world, providing clinical focus to ICT projects that will ensure the needs of the business are met with regards to patient care. The CCIO is the Medical Director/Caldicott Guardian.

6.8 The **Data Protection Officer (DPO)** has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate. The DPO is responsible for challenging and advising the Board on data protection to ensure that the Trust remains compliant.

6.9 The **RA Manager** means an individual appointed by the executive management team (EMT) of an organisation to set up and run the organisation's Registration Authority processes and procedures. They are responsible for ensuring good governance, and report annually to the organisation’s EMT on RA activity. In addition, they are required to undertake appropriate training to discharge these responsibilities and arrange training for all other RA team members. They are also authorised to verify and create identities, create and assign authenticator tokens, assign access permissions to a user, and perform advanced activities such as position creation and batch access management.

6.10 The role of the **Information Asset Owner** (IAO) will be assigned to staff that hold the position of Deputy/Associate Director, Head of Department, Service Delivery Group Manager. The IAOs will be accountable to the Senior Information Risk Owner (SIRO); and will have delegated responsibility from the SIRO to oversee and support the information risk management framework within their respective areas. The role will support the SIRO in fostering a culture that values, protects and uses information for the benefit of patients, service users, employees and the Trust as whole.

6.11 The Information Asset Owner may nominate an **Information Asset Administrator (IAA)** and delegate the day-to-day responsibility of the information asset. The IAO will nominate an appropriate person to undertake the role of **Data Protection Liaison Officer (DPLO)**.

6.12 The **Data Protection Liaison Officer (DPLO)** is responsible for providing administrative support to staff within the respective services/departments in the disclosure of personal data under the Data Protection legislation.

6.13 The **Head of Information Governance** is responsible for the day-to-day operational monitoring of information governance and information handling.

6.14 The **IT Service Manager** is responsible for the day-to-day management and operation of the corporate network infrastructure including the secure operation of the network, devices, connections, monitoring, protection and controls.

6.15 A **Safe Haven function** will be established in all services, teams and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information; such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g. Trust premises or a virtual location e.g. MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.

6.16 The **Head of Clinical Governance** is responsible for providing support to staff and managers who are responsible for information assets. They will provide support to the relevant groups and committees, including risk registers and monitoring service delivery risks.

6.17 The **Freedom of Information Manager** will ensure that the Trust complies with the Freedom of Information Act 2000 in processing Freedom of Information requests and the maintenance of a Publication Scheme. This role will manage the need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. Advising the organisation with regards to deciding whether the information can be released without infringing the UK GDPR and DPA 2018 data protection principles.

6.18 **All Line Managers** are responsible for ensuring that staff with responsibilities set out in this policy can undertake the role sufficiently, including training, to meet the organisation's obligations under the Data Protection legislation.

6.19 **All Staff** are responsible for upholding Data Protection requirements, including identifying and managing risk, and understanding/complying with relevant policies and procedures for handling personal data appropriate to their role. Staff must immediately report any event or breach affecting personal data held by the organisation to their Line Manager.

7 The Data Protection Principles

7.1 We will always comply with the UK GDPR data protection principles in respect of all personal data processed by the Trust. This includes personal data relating to all staff as set out under the Applicability section.

7.2 Accountability requires the Trust to take responsibility for what we do with personal data and how we comply with the other principles. There must also be appropriate measures and records in place to be able to demonstrate compliance.

7.3 All personal data will be treated in line with the UK GDPR 7 Key Principles. All data will be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processes in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed.
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes.

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

The Trust shall be responsible for and will be able to demonstrate compliance with UK GDPR Key Principles.

The Trust does not use the lawful basis of consent when an alternative can be used. And in circumstances when this might be considered as the lawful basis staff must seek advice from the Information Governance Team to ensure that the data protection requirements can be met, and that local processes and procedures are in place to ensure compliance.

The Trust recognises that there is a distinction between personal data and sensitive personal data. Information that is deemed 'Special Category' is covered in Appendix 2 of this document.

The Trust recognises that it is important for staff to understand the Code of Confidentiality and guidance is set out in Appendix 3 of this document.

See also ICO guidance on the data protection principles.

8 Governance of Data Protection

8.1 We will maintain oversight and transparency in the management of personal data. We will meet the accountability duties through the maintenance of the following record-keeping systems:

ICO guidance on the right to be informed, on required documentation.

9 Data Protection by Design

9.1 We will apply Data Protection by Design principles to new systems and business processes in consultation with the Data Protection Officer on the acquisition and development of new information systems and on proposals for significant new business processes and change.

See ICO guidance on accountability requirements, and EDPB guidelines on Data protection impact assessments and high-risk processing.

10 Data minimisation and accuracy

10.1 The Trust will apply the Records Management Code of Practice to new systems and business processes, through consultation with the Data

Protection Officer, with regards to existing systems; and the acquisition and development of new information systems and on proposals for significant new business processes and change.

ICO guidance on data minimisation and accuracy.

11 Retention of Personal Data

11.1 The Trust will apply the Records Management Code of Practice to new systems and business processes, through consultation with the Data Protection Officer, with regards to existing systems; and the acquisition and development of new information systems and on proposals for significant new business processes and change.

11.2 Staff should refer to the Trust's Records Management Policy.

Also see relevant ICO Guidance.

12 Individual rights

12.1 We will ensure that individuals' rights over their personal data are respected. These rights include:

- the right to be informed that processing is being undertaken
- the right of access to one's own personal data and to specific information about the processing
- the right to object to and prevent processing in certain circumstances
- the right to rectify or restrict inaccurate data
- the right to erase data or to data portability in certain limited circumstances
- specific rights with regard to automated decision making

12.2 All requests made by individuals (staff, contacts or patients/service users) relating to their personal data rights must immediately be forwarded to the appropriate Service/Dept Data Protection Liaison Officer (DPLO) or you can send the request directly to the Data Protection Officer (DPO) - contact details on the DPO website page - who will ensure that appropriate actions are taken, and a response issued without undue delay and at least within one month. A register of DPLOs can be found here: DPLO Register.

Relevant ICO guidance and EDPB guidelines on Automated decision making and profiling.

13 Data Sharing

13.1 All staff/colleagues must adhere to the Data Sharing Code of Practice, developed by the Information Commissioner's Officer (ICO), and have a process in place to create, develop, review, approve and sign Data Sharing Agreements that we establish with other data controllers.

13.2 In conjunction with others involved in establishing Data Sharing Agreements, the Data Protection Officer will review all Data Sharing Agreements before formal approval and sign-off by the Senior Information Risk Owner and/or the Caldicott Guardian.

13.3 The register of Data Sharing Agreements will be regularly reviewed and maintained by the Information Governance Team in conjunction with the key contacts.

13.4 The organisation will use the Information Sharing Gateway (ISG) as the technical for managing Data Sharing Agreements, including measuring risk.

Relevant ICO Guidance Data sharing information hub | ICO

14 Anonymised and Pseudonymised Information

14.1 The Data Protection Act 2018, the Human Rights Act 1998 and the common law relating to confidentiality apply to all organisations. This legislation requires that only the minimum personal data are used to satisfy any particular purpose.

14.2 The key principle is to ensure that, as far as is practicable, individual service users cannot be identified from data used to support purposes other than their direct care or to quality assure the care provided.

14.3 Anonymisation means that individuals are not identifiable and cannot be re-identified by any means reasonably likely to be used (i.e. the risk of re-identification is sufficiently remote). Anonymous information is not personal data and data protection law does not apply.

14.4 Pseudonymisation means that individuals are not identifiable from the dataset itself but can be identified by referring to other information held separately. Pseudonymised data is therefore still personal data and data protection law applies. Pseudonymisation is a method which disguises the 'real world' identity of patients by creating a pseudonym for each patient.

14.5 Effective Pseudonymisation processes depend upon robust Information Governance and effectively trained staff who understand the importance of data protection and confidentiality. The overall aims of pseudonymisation are to enable:

- The legal and secure use of patient data for secondary purposes by the NHS
- NHS business to no longer use identifiable data in its non-direct care related work wherever possible.

14.6 A Safe Haven function will be established in all services, teams and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information; such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g. Trust premises or a virtual location e.g. MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.

15 Data flows

15.1 In 2011 NHS organisations were required to complete a data flows transition and are now required to follow the NHS Digital and NHS England guidance, further information on the key points can be found at:

- NHS England s251 support for commissioning (https://www.england.nhs.uk/ig/in-val/)
- Safe Havens (https://www.digital.nhs.uk)
- Data Collections and data sets (https://www.digital.nhs.uk/data-and-information/datacollections-and-data-sets)
- Reference to Section 251: Control of patient information can be found under the legislation for the NHS Act 2006 at: http://www.legislation.gov.uk/ukpga/2006/41/section/251

15.2 The Head of Information Governance and the Information Programme Manager are responsible for working with service/department managers to develop an electronic record e.g. register, that details each use or sharing of personal information, including the legal basis of the processing and if applicable, whether the National Data Opt-Out (NDOO) has been applied to any sharing of the data for secondary purposes.

16 Sharing Data for Planning and Research Purposes

16.1 The National Data Opt-Out (NDOO) was introduced on 25 May 2018, enabling patients to opt-out from the use of their confidential patient information being used for research and planning, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

16.2 The Trust is compliant with the National Opt-Out Programme and has a process in place to receive requests for information. Staff that are involved in Planning and Research can contact the IG Team for advice and support to activate this process.

16.3 The Standard Operating Procedure can be found on SharePoint under IG Resources.

16.4 Further national details can be found here: National Opt-Out Programme

17 Training, Learning, Advice and Guidance

17.1 In addition to mandatory training all staff that undertake a role as set out in the Information Governance suite of policies under Roles and Responsibilities. Staff will be required to complete appropriate role-based training, conferences, webinars, development and specialist training as identified in the annual Learning Needs Analysis (LNA).

17.2 Staff will be required to seek appropriate advice, guidance and support from the nominated Information Asset Owners (IAO) and/or the Information Asset Administrators, or other roles defined in the related suite of policies. Staff will have a good understanding of the compliance requirements as set out in national guidance, legislation and local policies and procedures, such as technical and organisational data security and protection measures.

18 Data Security Incidents

18.1 Any security incidents which may impact on the confidentiality, integrity or availability of personal data held by the organisation and must be reported immediately to the Data Protection Officer via the Trust’s Incident Reporting system Datix.

18.2 Such events could include:

- Loss of records, laptops or media containing personal data
- Unauthorised access to information systems containing personal data
- Access of personal data with no justifiable business need
- Personal data being misdirected to an incorrect recipient
- Loss of access to systems containing personal data

18.3 All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

18.4 The Data Protection Officer will consider whether the incident meets the UK GDPR and DPA 2018 definition of a "personal data breach" which presents a risk to individuals. He/she will present a report to the Senior Information Risk Owner including a recommendation on whether to report the matter to the Information Commissioner's Office.

18.5 If the Senior Information Risk Owner decides that an incident constitutes a reportable data breach, the Data Protection Officer will report the incident to the Information Commissioner's Office (ICO) and liaise as appropriate.

18.6 If a data breach presents a high risk to the data subjects, the Data Protection Officer will ensure that they are also notified of the breach.

18.7 The Trust takes any data breach seriously. Any breach of the Data Protection Act 2018 constitutes a serious disciplinary offence. All breaches of Information Security, including near miss events, must be communicated to the relevant Information Asset Owner (IAO) and to the SIRO".

18.8 For further detail see the Personal Data Incident and Breach Reporting Procedure: European Data Protection Board Guidelines on Personal Data Breach Reporting and relevant ICO Guidance.

19 Data Protection Impact Assessments (DPIAs)

19.1 A Data Protection Impact Assessment (DPIA) is a process to help organisations identify and minimise the data protection risks of a project. Employees shall complete a DPIA when seeking to process information that is likely to result in a high risk to individuals. To assess the level of risk, both the severity and likelihood of any impact to an individual/s should be considered. The Employee should ask the Data Protection Officer (DPO) for their advice on the DPIA and document it as part of the process.

20 Privacy Notice and Fair Processing

20.1 The UK GDPR requires that data controllers provide certain information to people whose data they hold and use. This is known as a Privacy Notice (PN).

20.2 The Trust shall provide PNs to all patients and all Employees, identifying who the data controller is, including contact details for the DPO. The PN should also explain the purposes for which personal data is collected and used, how the data is used and disclosed, how long it is kept, and the controller's legal basis for processing.

20.3 A Statement of Fair Processing/PN will also be provided on the Trust's website. This reflects the requirement for a Statement of Fair Processing set out in the recommendations of the Caldicott Review.

21 Network and Information Systems Regulation (NISR)

21.1 The Trust applies The Networks and Information Systems Regulation (NISR) to all its operations. The NISR aims to raise the levels of overall security and resilience of network and information systems for Operators of Essential Services across the UK and defines a set of principles used to guide decision-making. These principles fall under four main objectives:

- **Managing the Security Risks**: by ensuring appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services
- **Protecting Against Cyber Attacks**: by ensuring proportionate security measures are in place to protect essential services and systems from Cyber attack
- **Detecting Cyber Security Events**: by ensuring security defences remain effective and detecting Cyber Security events affecting, or with the potential to affect, essential services
- **Response and Recovery Planning**: having capabilities to minimise the impact of a Cyber Security incident on the delivery of essential services including the restoration of those services where necessary.

22 Contact

Any questions about this policy should be directed to the Data Protection Officer. Contact details are on the Data Protection Officer website page.

23 Review and Maintenance

23.1 This Policy shall be reviewed every two years or in response to significant changes due to security incidents, variations of law and/or changes to organisational or technical infrastructure'.

23.2 This Policy is authored by the Head of Information Governance/DPO and maintained by the SIRO on behalf of the Board. Questions relating to its content or application should be addressed to the Trust see contacts section above.

Appendix 1 - Data Security and Protection Assurance Framework

As set out in the Terms of Reference

Appendix 2 - Special Categories Data Policy

Definitions

The Trust defines **Personal Data** as:

> "Information that relates to an identified or identifiable individual. An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals."

Common means of identifying someone may include, for example:

- name
- date of birth
- identification numbers
- bank details
- addresses, including email addresses
- other location data, such as an IP address
- online identifiers

We recognise our duties to protect all personal data but, in particular, **Special Category Personal Data** as defined in Article 9 of GDPR:

a) Personal data revealing a person's:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

b) Processing of

- genetic data
- biometric data
- health data
- sex life data
- sexual orientation data

In addition, we recognise the sensitivity and need to protect personal data relating to individuals' **criminal convictions and offences**.

Any proposed new use of Special Category Data must be subject to a Data Protection Impact Assessment and advice from the DPO.

For all uses of Special Category Data relying on the substantial public interest conditions in Schedule 1 of the DPA 2018 (see below), the processing must be included in our Record of Processing Activity (ROPA) maintained under Article 30 of GDPR. This will include a description of the lawful basis of processing (Article 6) and confirmation that the appropriate data retention rules are being applied.

Summary of description of data processing

A brief description of each category of Special Category data processed is given below:

Category	Special Category	Information Asset
Employment	data is processed for the purposes of employing healthcare staff clinical and non-clinical. Including DBS checks and Anti-fraud data processing	Electronic Staff Record (ESR)
Health	data is processed for the purposes of providing healthcare services to the population of Shropshire and Telford and Wrekin.	Primary Electronic Patient Record (EPR); and other clinical systems

See ICO Guidance on special category data and Schedule 1 of the Data Protection Act 2018.

Appendix 3 - Code of Confidentiality Policy

Policy Statement

- People should feel confident that we handle confidential information appropriately. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out in this policy.
- As an organisation that collects, analyses, publishes or disseminates confidential health and care information we must follow the NHS Code of practice on confidential information.
- We will define the steps that we must, should and may take to ensure that confidential information is handled appropriately.
- In accordance with the NHS Code of practice on confidential information we will put the right structures and procedures in place so that all staff follow the confidentiality rules.
- The policy will set out the expectations of the Trust to those responsible for setting and meeting organisation policy on the handling of confidential health and care information, such as Board members.
- The 'Confidentiality: NHS Code of Practice' sets out standards to ensure that patient information is handled fairly, lawfully and as transparently as possible.
- Our staff and our colleagues who work within or under contract to NHS organisations must understand and refer to the legal requirements and best practice contained in this policy.

Link here: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

What is Confidential Information

- Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient health information, employee records, occupational health records, etc. It also includes Trust confidential business information.

The Caldicott Principles

- Whether you are requesting, using or disclosing confidential information staff should at all times abide by the 8 Caldicott Principles as set out in the list below. Further information is available on the Trust website here:

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

The Confidentiality Model

In accordance with the NHS Code of practice on confidential information staff will adhere to the four main requirements:

- **PROTECT** – look after the patient's information
- **INFORM** – ensure that patients are aware of how their information is used
- **PROVIDE CHOICE** – allow patients to decide whether their information can be disclosed or used in particular ways
- To support these three requirements, there is a fourth:
- **IMPROVE** – always look for better ways to protect, inform, and provide choice

The Trust Definition of Confidential Information

- Confidential information can be anything that relates to patients, staff (including volunteers, bank and agency staff, locums, student placements), their family or friends, however stored. For example, information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, mobile phones, and digital cameras.

- It can take many forms including medical notes, audits, employee records, occupational health records etc. It also includes any confidential information relating to another organisation. This will include other NHS Trusts, independent contractors (GPs, dentists, pharmacists and optometrists) and local authorities (e.g. social care, education etc.).

- Personally identifiable information (PID) is anything that contains the means to identify a person, especially when used in combination, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

- Certain categories of information are legally defined as particularly sensitive and are carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

- During your duty of work you should consider all information to be sensitive, even something as simple as a patient's name and address. The same standards should be applied to all information you encounter.

Duty of Confidence

- All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the Data Protection Act 2018, UK GDPR and, in addition, for health and other professionals through their own professions Code(s) of Practice/Conduct. The term employee is considered to include all non-employed workers e.g. temporary staff, agency workers, students and secondments from other organisations.

- This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with other information which should also be treated with the same degree of care e.g. business in confidence information, patient referral letters, discharge summaries, waiting list data, consultant's workloads, clinic lists.

- Disclosures and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and government guidelines.

- The principle behind this Code of Practice (Code) is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Organisation's security systems or controls to do so.

Notes:

1. Although these were drawn up specifically to protect patient information they are just as applicable to the use or disclosure of all personally identifiable information (PID).
2. These principles should be considered as a simple checklist which you can look back to if ever you are challenged over your use or disclosure of confidential information.

Seven Golden Rules for Information Sharing

1 Remember that the Data Protection Act 1998, UK GDPR, the Caldicott Principles, and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately

2 Be open and honest with the individual (and/or their family where appropriate) from the outset about the why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so

3 Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible

4 Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgment on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared

5 Consider safety and wellbeing: Base your information sharing decisions on considerations of the safety and wellbeing of the individual and others who may be affected by their actions.

6 Necessary, proportionate, relevant, adequate, accurate, timely and secure: Ensure that information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely

7 Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose

Disclosure of Confidential Information

- Remember your duty of care. This means that where you have control of personal information about patients and staff, you must not allow anyone access to the data for any purpose, unless the person has been properly trained and authorised by the Trust, an NHS Trust or comparable body and is subject to a duty of confidentiality in their employment, or because of their registration with a statutory body.

- Never give out information to persons who do not “need to know” in order to provide health care and treatment.

- All requests for patient identifiable information should be justified. This applies whether the request comes from within the Trust or from someone outside the Trust. Some requests may need to be agreed by the Trust’s Caldicott Guardian.

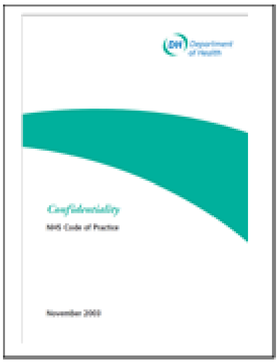
- The Department of Health Confidentiality Code of Practice should be read in conjunction with this Policy. For example, areas such as:
    - ➢ Disclosure of information to other employees of Shropshire Community health NHS Trust
    - ➢ Joint health/social care teams e.g. substance misuse or community health services
    - ➢ Acute Trusts or NHS organisations
    - ➢ Disclosures in the public interest
    - ➢ Serious crime
    - ➢ Risk of harm
    - ➢ Requests for information by the Police
    - ➢ Requests for information by the Media
    - ➢ Safeguarding,

If in doubt, check with your manager or the health professional in charge of the patient’s care.

Governance of Confidentiality

- The Trust will maintain oversight and transparency in the management of confidentiality. We will meet our accountability duties through the policies and procedures that we have in place for data security and protection.

- All staff will receive annual data security and protection training.



- Incidents will be monitored and managed through the incident reporting procedure.

- A **Safe Haven function** will be established in all services, teams and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information; such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g. Trust premises or a virtual location e.g. MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.

- All information exchanges between providers and purchasers as part of the contracting process will be assessed in line with national guidance. In the absence of national guidance local processes will be agreed.