Shropshire Community Health NHS Trust

Individual Rights Policy

(Including Subject access requests)

Controlled document

This document is uncontrolled when downloaded or printed.

Author(s) **Owner(s)**	Author: Gill Richards, Associate Director of Governance Owner: Shelley Ramtuhul, Director of Governance/Senior Information Risk Owner (SIRO)
Version No.	Version 0.2
Approval Date	June 2023
Review Date	June 2026

Document Details	
Title	Individual Rights Policy
Trust Ref No	2259-83297
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	Associate Director of 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	
Full Equality Impact Assessment	
Lead Director	Director of Governance/Senior Information Risk Owner (SIRO)
Category	General
Subcategory	Information Governance
Review date	16 June 2026
Distribution	
Who the policy will be distributed to	The Head of Information Governance will submit this document to the Risk Management Team for publication on the Trust's public website and Staff Zone. The IG Team will notify all Data Protection Liaison Officers (DPLOs) of the publication of this policy
Method	Website, email, 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	
1	17/03/2023	New policy.
2	07/03/2024	Updated: IG job titles and contact details.
3		
4		
5		
6		

This copy is uncontrolled unless printed on 'Controlled' paper.

CONTENTS

Table of 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 and procedures can be found in the Trust's document Library and IG resources on Public Website and Staff Zone

- Data Protection Policy
- Information Security Policy
- Information Registers
- 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

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 role of the **Information Asset Owners (IAOs)** will be assigned to appropriate senior managers with accountability to the Senior Information Risk Owner. They have delegated responsibility from the SIRO for managing risks to their assets and are accountable for:

- ensuring that all systems, processes, records, and datasets within their business area is compliant with this policy and with Data Protection legislation.
- assisting the Data Protection Officer in their duties through providing all appropriate information and support

- ensuring that their staff are aware of their data protection responsibilities.
- consulting the Data Protection Officer on new developments or issues affecting the use of personal data in the organisation
- ensuring Data Protection Impact Assessments (DPIAs) are conducted as appropriate on data processing activities in their business area, drawing on advice from the Data Protection Officer. IAOs must ensure that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO, and following the Trust risk strategies, policies, code of practice and procedures.
- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset.
- know who has access to the asset (whether system, portable technology, or information) and why, and ensure access is monitored and compliant with Policy.
- understand and address risks to the asset.
- foster a culture that values, protects, and uses information for the benefit of patients, Employees, and the Trust as whole
- provide assurance to the SIRO on the security and use of information assets.
- advise the SIRO regarding Business-Critical Information Assets in keeping with the Information Risk Management Policy and Business Continuity and Disaster Recovery – Information Security Policy.
- to comply with the Data Security and Protection Toolkit (DSPT) Standards 1-10 with regards to the information asset, including responding to requests for documented evidence as part of the annual assessment. Guidance here: Help (dsptoolkit.nhs.uk)
- to undertake regular audits with regards to the compliance of the Data Security and Protection Toolkit (DSPT) annual assessment and document the findings and outcomes.
- Ensuring a Data Quality Procedure (DQP) is completed for each asset, in accordance with the Information Quality Assurance Policy. The DQP is to be uploaded into the Information Asset Register entry for that asset.

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

6.11 **Data Protection Liaison Officers (DPLOs)** are responsible for providing administrative support to staff within the respective services/departments in the disclosure of personal data under the Data Protection legislation.

6.12 The **Head of Information Governance** is responsible for the day-to-day

operational monitoring of information governance and information handling.

6.13 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.

6.14 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.

6.15 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.

6.16 The **Freedom of Information Manager** to 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.

6.17 **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.

6.18 **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 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.

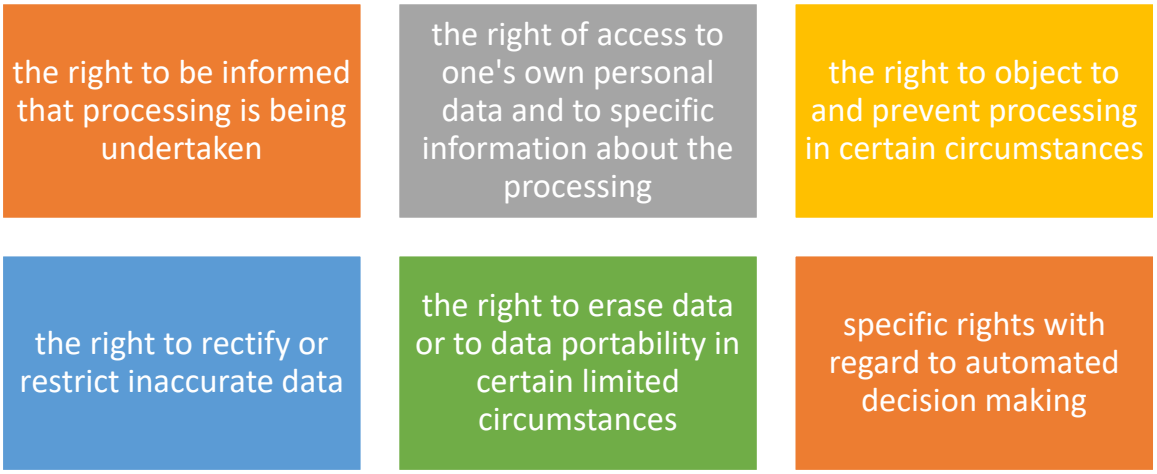
See also ICO guidance on the data protection principles.

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:

9 Individual rights

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



Individual rights are listed in full below:

9.2 The **Right to be informed**: we will ensure that we keep patients, service users and staff informed about the collection and use of their personal data. We will use methods that are concise, transparent, intelligible, easily accessible and will use clear and plain language. We will provide information through the use of relevant Privacy Notices on the public Website; through service leaflets and correspondence; and verbal communication e.g. clinical settings. We will respond to the request within one calendar month. Right to be informed | ICO

9.3 The **Right of access**: we will ensure that we have a process in place to receive requests, in writing, verbally and through social medial, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right of access | ICO

9.4 The **Right to rectification**: we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right to rectification | ICO

9.5 The **Right to erasure**: we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right to erasure | ICO

9.6 The **Right to restrict processing**: we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right to restrict processing | ICO

9.7 The **Right to data portability:** when applicable, we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right to data portability | ICO

9.8 The **Right to object**: we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Right to object | ICO

9.9 **Rights related to automated decision making including profiling**: when applicable, we will ensure that we have a process in place to receive requests, in writing and verbally, from patients, service users, staff and other third parties such as relatives, carers and solicitors. We will escalate complex requests to the Caldicott Guardian or the Senior Information Risk Owner (SIRO) and seek advice and approval when required. We will respond to the request within one calendar month. Rights related to automated decision making including profiling | ICO

9.10 Requests made by individuals (staff, contacts or patients/service users) relating to their personal data rights must be sent directly to the relevant service Service/Dept marked “For the Attention of the Data Protection Liaison Officer (DPLO)” or requests can be sent directly to the Data Protection Officer here: Shropcom.sar@nhs.net

9.11 We have a documented process for handling requests that is available in the Trust’s Document Library.

Also see relevant ICO Guidance.

Training, Learning, Advice and Guidance

9.12 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, will

be required to complete appropriate role-based training, conferences, webinars, development and specialist training as identified in the annual Learning Needs Analysis (LNA).

9.13 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.

10 Data Security Incidents

10.1 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. 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

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

10.3 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.

10.4 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.

10.5 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.

10.6 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".

10.7 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**.

11 Privacy Notice and Fair Processing

11.1 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).

11.2 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.

11.3 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.

12 Contact

Any questions about this policy should be directed to:

Data Protection Officer, Shropshire Community Health NHS Trust,
Governance Directorate, Ground Floor, Left Wing, Mount McKinley, Shrewsbury Business Park, Anchorage Avenue, Shrewsbury, SY2 6FG

Email: **shropcom.IGQ@infreemation.co.uk**

Tel: 01743 277500 Trust main switchboard

13 Review and Maintenance

13.1 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'.

13.2 This Policy is authored by the Head of Information Governance/Data Protection Officer 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.