Shropshire Community Health
NHS Trust

Records Management and Security Policy

Controlled document
This document is uncontrolled when downloaded or printed

Author(s) Owner(s)	Author: Information Governance Manger Owner: Associate Director of Governance
Version No.	Version 3.0
Approval Date	December 2024
Review Date	December 2027

Document details	
Title	**Records and Document Management Policy**
Trust Ref No	1348
Local Ref (optional)	3.0
Main points the document covers	This policy explains how the records and document management arrangements will be delivered and adhere to the national Code of Practice.
Who is the document aimed at?	All staff (including employees, contractors, temporary staff, secondments, student placements)
Owner	Associate Director of Governance
Approval process	
Who has been consulted in the development of this policy?	A selection of Managers/staff
Approved by (Committee/Director)	Data Security and Protection Assurance Group
Approval Date	Jan 2025
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Director of Governance
Category	General
Subcategory	Information Governance
Review date	Jul 2027
Distribution	
Who the policy will be distributed to	All staff (including non-employed workers)
Method	Website and email
Keywords	Records management, records, record keeping, archive, archiving, disposal, retention, retention schedule, corporate, clinical, filing, archiving, storage, data protection, freedom of information, information governance, NHS number.
Document Links	
Required by CQC	Yes – Well Led
Other	Data Security and Protection Toolkit (DSPT)
Amendments History	

No	Date	Amendment
1.	May 2012	Policy reviewed and updated to reflect changes within the Trust's organisational structure and latest guidance and standards
2.	Aug 2013	Changes to contact details for the Information Governance and Data Protection Lead
3.	Nov 2014	Review and minor amendments to reflect current organisational structure and links to reference information
4.	Mar 2017	Review and minor amendments to reflect current organisational structure and links to reference information
5.	Oct 2018	Review and update to take into account new Data Protection legislation – DPA and GDPR Combine the previous separate Records Retention Archiving and Disposal Policy into this policy
6.	Dec 2021	Templar Executive Consultancy and IG Manager. The whole document was reviewed by a consultancy and finalised by the IG Manager.
7.	Jan 2022	Updated to reflect the transfer of the Records Management role into IG. Processes have been extracted into a new SOP.
8.	July 2022	Update IT Service Manager description
9.	October 2022	Update Owner - Corporate Secretary/Director of Governance/Senior Information Risk Owner (SIRO)
10.	March 2023	Amended 'Information Governance Manager' to 'Head of Information Governance'. Updated Safe Haven role to function. Updated IAO role (detailed moved to new Appendix 2). Updated role of Information Risk Manager to include assigned to Head of IG. Added 'Records of historical value'. Updated references 'Records Management Group'. Naming conventions advice updated - 11.1,(d)(f).
11.	May 2024	Revised policy statements and extracted items that are part of the Standard Operating Procedure (SOP)

Contents

1 Policy Statement

1.1 This policy relates to records and document management for Shropshire Community Health NHS Trust (hereafter referred to as the Trust); and includes reference to the security of records and documents.

1.2 The Board recognises that records and document management is an important part of healthcare and corporate services. Understanding and working within the NHS Records Management Code of Practice 2021 is at the core of protection the information that drives and supports its business.

1.3 The Records Management Code of Practice 2021 states that, *"All health and care employees are responsible for managing records appropriately and must manage them in accordance with the law. The Public Records Acts 1958-1967 are the principal legislations relating to public records. Records of NHS organisations are public records in accordance with Schedule 1 of the 1958 Act. This means that employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations."*

1.4 The Trust is highly reliant on information that is captured, stored, processed and delivered by information systems and their associated communication facilities.

1.5 Such information plays a vital role in supporting businesses processes and patient services, in contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.

1.6 The key requirement of this policy is for records and documents to be managed in a robust way within work areas; and must not be seen as something that is the sole responsibility of the information governance staff and is part of everyday practice by all staff members.

1.7 The Trust recognises that good record keeping is also important to achieve compliance with the following legislation and regulatory requirements:

- The Data Protection Act 2018 (DPA)
- UK General Data Protection Regulation
- The Freedom of Information Act 2000 (FOI)
- The Access to Health Records Act 1990
- The Public Records Act 1958 and 1967
- Care Quality Commission (CQC) Fundamental Standards
- Data Security and Protection Toolkit
- Mental Capacity Act 2005
- Accessibility Information Standard 2016 (AIS)

See Appendix 2 for a brief summary of the items listed above.

1.8 The Records Management Code of Practice has been published by NHSX and provides guidance on how to keep records, including how long to keep different types of records. The Code provides a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational, and individual responsibilities when managing records.

2 Purpose

2.1 This policy defines how the Trust will manage records and documents and how the effectiveness will be assessed and measured.

2.2 This policy explains the document and records management arrangements adopted within the Trust. It covers records prepared and maintained in all media, including paper and electronic records, for the benefit of all of Trust's stakeholders.

2.3 It is the policy of the Trust to ensure that the approach to records and document management, includes:

- **Records are available when needed:** from which the Trust is able to form a reconstruction of activities or events that have taken place
- **Records can be accessed:** records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist (clear version control process)
- **Records can be interpreted:** the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records
- **Records can be trusted:** the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated
- **Records can be maintained through time:** the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format
- **Records are secure:** from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails will track all use and changes.
- **Records are held in a robust format**; which remains readable for as long as records are required
- **Records are retained and disposed of appropriately:** using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.

3 Scope and Applicability

3.1 This policy sets out the Trust's approach to records and document management and relates to electronic, paper-based, and other formats whether held in automated or manual systems, relating (but not limited to):

- patient/ client / service user information
- staff personal information
- Trust business, commercial and operational information
- Research, audit and reporting information.

3.2 This policy is to ensure that all staff are aware of their individual responsibilities in relation to records and document management as set out under the Legal and Regulatory requirements in 1.8.

3.3 This policy applies to all Trust staff (including temporary workers, locums and staff seconded or contracted from other organisations) and parties authorised by the Trust together with their staff (including temporary workers, locums and staff seconded or contracted from other organisations).

4 Related Documents

4.1 This policy should be read in conjunction the documents set out below and other Trust processes and procedural documents:

- Records Management and Security Procedures
- Clinical Record Keeping Guidelines
- NHS Number Retrieval, Verification and Use Procedure
- Policy approval and ratification framework
- Information Security Policy
- Data Protection Policy (incorporating Confidentiality, and Special Categories)
- Individual Rights Policy (including Subject Access Requests)
- Information Quality Assurance Policy
- Information Risk Policy
- Incident Reporting Policy
- Mandatory Training Policy and Procedure
- Accessible Information Standard Policy
- Waste Management Policy
- Freedom of Information Policy
- Management of Personal Files Policy

5 Responsibilities

5.1 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

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

5.3 **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.

5.4 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.

5.5 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.

5.6 The Trust 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.

5.7 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 Associate Director of Digital Services.

5.8 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**.

5.9 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.

5.10 **Directors, Deputy Directors, Divisional and Operational Managers** of services and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their service are managed in a way which meets the aims of the Trust's records management policies.

Commented [SD(CHNT1]: Hi @RICHARDS, Gill, I think we need to change this to 'Operational Leads'?

5.11 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.

5.12 The role of the **Information Asset Owner (IAO)** will be assigned to staff that that are members of the Senior Leadership team (SLT). 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. Full responsibilities as set out in the Information Risk Policy.

Commented [DS2]: @RICHARDS, Gill (SHROPSHIRE COMMUNITY HEALTH NHS TRUST) this paragraph needs to be reviewed.

5.13 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).

5.14 **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.

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

5.16 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.

5.17 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 Information Governance Team.

5.18 The **Information Risk Manager** 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. The role of the Information Risk Manager will be undertaken by the Associate Director of Governance.

5.19 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.

5.20 **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.

5.21 The role of **custodian of records and documents** will be undertaken by the Information Asset Owners and Information Asset Administrators.

5.22 The role of **Records Manager** will be undertaken by the Associate Director of Governance and the function will be provided by the Information Governance Manager and the Information Governance Team; responsibilities will include:

- Development and maintenance of the Records and Document Management Policy and compliance;
- the overall development and maintenance of a records management framework that is aligned to the information risk management framework;
- providing learning and development with key learning points from this policy and for monitoring compliance with the policy to assess its overall effectiveness.
- developing and supporting a culture of high-quality records management practice across the Trust to deliver associated organisational benefits.
- knowing what records the Trust holds and where they are through audits, assessments, and spot checks.
- ensuring that records created by the Trust are stored securely and that access to them is controlled

5.23 Under the Public Records Act 1958 the responsibility of the Chief Executive and senior managers for the safe keeping of records is extended to all staff for all records they either create, use or handle.

5.24 All staff who come into contact with patient or personal information are subject to a Common Law Duty of Confidentiality. This duty of confidentiality continues beyond the death of a patient or after an employee has left the NHS.

5.25 The Data Security and Protection Assurance Group (DSPAG) will act as the forum for ensuring that compliance is achieved with the relevant legislative and regulatory standards and will report to the Digital Programme Group (DPG) Relevant risks and issues will be escalated to the Quality and Safety Committee and/or the Resource and Performance Committee.

5.26 **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.

6 Caldicott Principles

6.1 To ensure that people's information is kept confidential and used appropriate the Trust will adhere to the Caldicott Principles.

7 Creating, locating, and retrieving records

7.1 The Trust will have procedures in place to appropriately classify, tittle and index new records in a way that facilitates management, retrieval, and disposal.

7.2 A central information asset register will be developed, maintained, and managed to identify where we use manual and electronic record-keeping systems.

7.3 The whereabouts of records will be tracked with regards to their movements and attempts to trace records that are missing or not returned will be made.

7.4 There will be an index of records stored off-site with unique references to enable accurate retrieval and subsequent tracking.

7.5 Staff will be responsible for managing records to ensure they can respond to requests and disclosure information under the data protection and freedom of information legislation.

7.6 The Trust will have a procedure for the use of the NHS Number to retrieve and verify patients.

7.7 The Trust will use a unique identifier for staff records.

8 Specific types of records

8.1 Staff will be responsible for setting out procedures in accordance with this policy to ensure that specific types of records, that are applicable to the Trust, are managed in accordance with the Records Management Code of Practice.

8.2 A list of records is set out in Appendix 1. The procedures will be held in a central library and made available to all staff.

9 Other types of records

9.1 For records that are not about staff or patients, for example, board minutes or records relating to buildings, there will be procedures in place to manage those records.

10 Electronic Patient Record (EPR) systems

10.1 Electronic records provide health and care professionals with access to critical information when needed, enabling them to deliver better care. They are also an important foundation for service transformation and integration. The Trust will develop plans to make better use of digital technology as set out in the NHS long term plan.

10.2 Paper records will only be held where there is no digital alternative.

11 Security for transfers

11.1 The Trust will have documented guidelines to protect the internal and external transfer of records by post, and electronically.

11.2 Staff will minimise data that is transferred off-site and keep it secure in transit.

11.3 When data is transferred off site, staff will use an appropriate form of transport (for example NHS Mail, secure courier, internal transport, encryption, secure file transfer protocol (SFTP) or Virtual Private Network (VPN)) and will make checks to ensure the information has been received.

11.4 There will be agreements in place with any third parties used to transfer business information between the Trust and third parties.

Commented [SD(CHNT3]: @RICHARDS, Gill (SHROPSHIRE COMMUNITY HEALTH NHS TRUST) I have added this in relation to the complaint from another Trust about an individual wanting the Trust to retain their records on paper. Is this sufficient?

Commented [RG(CHNT4]: Guidance on data transfer is needed for this section.

Commented [SD(CHNT5R4]: Raise with GR to check this meets expectation?

12 Data quality

12.1 The organisation has an Information Quality Assurance policy.

12.2 Staff within the organisation are required to review the policy as part of their induction checklist.

12.3 Roles and responsibilities are clearly defined within the policy.

13 Audits and Assessment

13.1 In accordance with NHS guidance the Trust will comply with the audit and assessment requirements and document the findings and outcomes.

13.2 Information Asset Owners will assist with compliance and support the Information Governance team in providing evidence for the Data Security and Protection Toolkit (DSPT) annual assessment.

14 Retention schedule

14.1 Records and documents will be retained in accordance with the Records Management Code of Practice (RMCoP). The RMCoP retention schedule is available to staff, patients, and service users.

14.2 The Trust will have a centralised and documented retention schedule based on business needs that references national, local and statutory requirements and other principles, for example National Archives.

14.3 The schedule will provide sufficient information to identify all records and to implement disposal decisions in line with the schedule.

14.4 Responsibilities will be appropriately assigned to key staff to make sure that all staff adhere to the schedule and that it is reviewed regularly.

14.5 The Trust will regularly review retained data to identify opportunities for minimisation, pseudonymisation or anonymisation and will document this in the schedule.

15 Destruction and deletion

15.1 The destruction of paper records will be managed by a third-party supplier under a contract. The supplier will comply with cross shredding or incineration destruction regulations.

15.2 Any third-party supplier contracted by the Trust will provide assurance that they have securely disposed of the data. Regular checks will be conducted through audit checks and destruction certificates.

15.3 Staff will either hold, collect or securely store, confidential waste awaiting destruction.

15.4 There will be a record of all equipment and confidential waste sent for disposal or destruction.

15.5 For electronic devices there will be a process in place that is compliant with data security and protection legislation.

Commented [SD(CHNT6]: DS to review

Commented [RG(CHNT7]: We will need guidelines on sending records to the National Archives.

Commented [SD(CHNT8R7]: I have added this to the SOP

Commented [SD(CHNT9R7]: Paragraph 33 in SOP

Commented [RG(CHNT10]: Do we have a log for this? If so where is it and who owns it?

Commented [SD(CHNT11R10]: I thought this was the ISP?

Commented [SD(CHNT12R10]: @RICHARDS, Gill, I have changed the word 'log' to "record".

Commented [SD(CHNT13R10]: The IG team maintains a log of the destruction of smartcards and ribbons. IT should have a log but we don't know if they do and where it is held.

16 Information Asset Register

16.1 The Trust will have a central asset register which holds details of all information assets (software and hardware) including:

- asset owners and administrators
- asset location
- retention periods; and
- security measures deployed.

16.2 The register will be maintained and managed by staff with specialist roles who have completed appropriate training. This will be reviewed periodically to make sure it remains up to date and accurate.

16.3 There will be a process in place to periodically risk-assess assets within the register and to conduct physical checks to make sure that the hardware asset inventory remains accurate.

17 Rules for acceptable software use

17.1 The Acceptable Use Policy will be included in the Trust's Information Security Policy.

17.2 There will be procedures to document the security arrangements and measures in place to protect the data held within each system or applications.

17.3 The Trust will monitor compliance with acceptable use rules and makes sure that staff are aware of any monitoring.

18 Access control

18.1 The Information Security Policy will set out the Access Control policy and specify that users must follow the Trust's practices in the use of secret authentication information, such as passwords or tokens.

18.2 The Trust will have a formal user access provisioning procedure to assign access rights for staff, including temporary staff, and third-party contractors to all relevant systems and services required to fulfil their role. This will be integrated into the joiner, mover, leaver process.

18.3 There is a process in place to restrict and control the allocation and use of privileged access rights, including a documented log of user access to systems holding personal data.

18.4 We will regularly review users' access rights and adjust or remove rights where appropriate, including when an employee changes their role or leaves the Trust.

19 Unauthorised access

19.1 The Trust has a process in place to restrict access to systems or applications processing personal data to the absolute minimum in accordance with the principle of least privilege.

Commented [RG(CHNT14]: Do we have this? Where is it?

Commented [ST15R14]: DS to check - Is this in the ISP>

Commented [SD(CHNT16R14]: @RICHARDS, Gill (SHROPSHIRE COMMUNITY HEALTH NHS TRUST) I have changed 16.2 to general statement.

Commented [RG(CHNT17]: Does IT do this?

Commented [SD(CHNT18R17]: @RICHARDS, Gill, yes.

Commented [RG(CHNT19]: Is this in the ISP?

Commented [SD(CHNT20R19]: @RICHARDS, Gill (SHROPSHIRE COMMUNITY HEALTH NHS TRUST) , Yes. They are mentioned throughout the policy.

19.2 In accordance with the Trust's Information Security Policy there will be processes and procedures in place to ensure that access to systems is authorised.

19.3 Access to Trust sites and secure locations will be restricted and managed to ensure that information is held securely.

20 Mobile devices, home or remote working and removable media

20.1 The Trust will have a policy in place that covers the use of mobile devices, homeworking, and remote working, and demonstrates appropriate protection and security is in place, and that the associated risks are managed.

21 Secure areas

21.1 The Trust will have policies and procedures in place to protect secure areas that contain either sensitive or critical information, that includes physical and digital controls.

21.2 All services, teams, and departments will establish a "safe haven" to protect information, in accordance with the information risk management framework and policy.

22 Business continuity, disaster recovery and back-ups

22.1 There will be a policy and procedure in place to manage risk-based Business Continuity Plans, including the management of disruption and a Disaster Recovery Plan to manage disasters, which identify records that are critical to the continued functioning of the organisation.

23 Data Losses and Confidentiality/Security Breaches

23.1 The Trust will have a policy and procedure in place for reporting incidents.

23.2 All data breaches will be reported through the incident reporting system as they occur. An investigation group will be established and include the Senior Information risk Owner (SIRO), Caldicott Guardian, Data Protection Officer (DPO) and the Information Asset Owner.

23.3 Serious incidents will be reported within 72 hours and managed in accordance with the data protection legislation and the Data Security and Protection Toolkit (DSPT).

24 Training and awareness

24.1 All staff (employed and non-employed) will be offered appropriate training through a variety of sources. The training requirements will be reviewed by the Associate Director of Governance as part of the annual Learning Needs Analysis LNA) and scoped as follows:

- Specialist roles e.g. Information Risk Management, Freedom of Information.
- Corporate induction
- Data Security Level 1 (mandatory)

- Awareness raising, and presentations.
- Policies and Standing Operating Procedures

24.2 In conjunction with all managers, specialist staff and staff with key roles, the author of this document will be responsible for ensuring that sufficient and adequate awareness is raised.

25 Data Protection Impact Assessments

25.1 Where there is a new or change in use of personal data and a potentially high risk to privacy, the Trust will have a process in place to conduct data protection impact assessments in accordance with the data protection legislation.

26 Inquiries

26.1 The Trust will have a procedure in place to manage inquiries in accordance with statutory requirements and national and local guidance.

27 Review and Monitoring

27.1 This policy will be reviewed by the author in accordance with the Policy Approval and Ratification Framework; or in response to changes due to security incidents, changes to the Trust's technical infrastructure, legislative amendments, or updates made to the Data Security and Protection Toolkit (DSPT).

27.2 The Data Security and Protection Assurance Group will review incidents for trends or patterns and impacts on controls in place and provide a commentary for an annual risk assurance report.

27.3 Any breach of or refusal to comply with this policy will lead to disciplinary action in accordance with the Trust's Human Resource and framework.

28 Microsoft 365 (N365)

28.1 **MS Teams**. All MS teams are to be requested and configured as per the Records Management and Security SOP.

28.2 **SharePoint Online**. All Trust business information is to be created and stored in SharePoint[1] as per the Records Management and Security SOP.

28.3 **OneDrive**. OneDrive is only to be used to create and store information that belongs to the user. OneDrive data is subject to NHS Mail retention policies and therefore is not suitable for storing business information that must be retained in accordance with the Records Management and Security SOP, Records Management Code of Practice, and local business administrative procedures.

28.4 **NHS Mail**. Outlook must not be used to store records that form part of the corporate/clinical record. Any emails that contain information of value to the organisation must be transferred to the primary record or document and

[1] Files shares can be used as an interim measure until migration has been completed.

records management system i.e. MS Teams or other incident/case/support management systems. Ownership of Group Mailboxes and Application Accounts are to be transferred to another Owner prior to leaving the service/department or the organisation.

29 Related documents

29.1 The following document(s) are related to this policy:

- Record Management and Security – SOP
- Record Management and Security – SOP - Archiving

Appendix 1 – Specific types of records

1.1 Procedures that are applicable to the Trust will be held in a central library on the Staff Zone.

1.2 List of procedures

- Adopted persons health records
- Asylum seekers records
- Audio and visual records
- Child school health records
- Complaints records
- Contract change records
- Continuing health care records
- Controlled regime
- Duplicate records
- Evidence required for courts
- Family records
- Integrated records
- Occupational Health records
- Pandemic records
- Patient or service user held records
- Patient or service user portals
- Pharmacy held patient records
- Prison health records
- Records relating to sexually transmitted diseases
- Staff records
- Transgender patient's records
- Protected persons health records
- Cloud-based records
- Email and record keeping implications
- Instant messaging records
- Integrated viewing and technology and record keeping
- Scanned records
- Social media
- Website as a business record

Appendix 2 – Reference documents

2.1 **References**. Staff should refer to the following guidance in conjunction with this policy. Some references have been used to develop this policy:

2.2 Some references have been used to develop this policy:

- Records Management Code of Practice: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/
- Data Protection legislation UK GDPR guidance and resources | ICO
- Freedom of Information legislation FOI, EIR and access to information | ICO
- Human Rights Act, 1998
- The Public Records Act, 1958 http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51
- The Access to Health Care Records Act, 1990 https://www.legislation.gov.uk/ukpga/1990/23/contents
- The Access to Medical Reports Act, 1988 https://www.legislation.gov.uk/ukpga/1988/28/contents
- Care Quality Commission: Fundamental standards - Good Governance (Regulation 17) http://www.cqc.org.uk/content/fundamental-standards
- Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/
- Data Security and Information Governance: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance
- NHS Confidentiality Code of Practice: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- The Care Record Guarantee: https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/8/care_record_guarantee.pdf
- NHS Choices – Your health and care records: http://www.nhs.uk/nhsengland/thenhs/records/healthrecords/pages/overview.aspx
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000: http://www.legislation.gov.uk/ukpga/2000/36/section/46
- The National Archives website: Standards and best practice for records managers – http://www.nationalarchives.gov.uk/information-management/projects-and-work/standards-records-managers.htm

2.3 **Related Documents**. Shropshire Community Health NHS Trust policies and procedures which relate to this policy include:

- Records Management and Security – Standing Operating Procedure

2.4 These documents are available on the Trust's public website and Staff Zone.

2.5 **Definitions**

Word	Definition/Explanation	Source
Active Record	A record that is still in use.	

Word	Definition/Explanation	Source
Appraisal	The process of evaluating an Trust's activities to determine which records should be kept, and for how long, to meet the needs of the Trust, the requirements of the Department of Health and Social Care and Data Protection Act.	
Archive	The term used when records are no longer active and are unlikely to require retrieval but are required to be retained until their disposal date.	
Caldicott Principles	Seven principles that should be followed when considering sharing confidential information, put together by Dame Fiona Caldicott following a review she carried out in regard to confidentiality in 1997 and update in March 2013 following the Information Governance (Caldicott 2) Review	
Classification	The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. (BS ISO 15489-1:2016)	NHS Code of Practice
Confidential waste	Includes any material that contains information that would identify an individual patient, employee or business sensitive information.	
Corporate Record	A document becomes a record when it has been finalised and becomes part of the Trust's corporate information (a document has content – a record has content, context & structure)	
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example paper to electronic).	National Archives
Disposal	The implementation of appraisal and review decisions. These comprise of the destruction of records and the transfer of custody of the records.	

Word	Definition/Explanation	Source
Electronic Staff Record (ESR)	This is the national, integrated Human Resources (HR) and Payroll system which will be used by all 600+ NHS Trusts throughout England and Wales.	Electronic Staff Record Website
Electronic Patient Record (EPR)	The Trust's main EPR is Rio	
Encryption	Encryption is the means of converting information using a code that prevents it being understood by anyone who isn't authorised to read it. Files, emails, even whole hard drives can be encrypted. As a general rule the more bits used for encryption the stronger it will be, so 128-bit is stronger that 64-bit.	Get Safe Online Organisation
Filing System	A plan for organising records so that they can be found when needed. (The National Archives, Records Management Standard RMS 1.1)	NHS Code of Practice
Inactive Record	A record no longer being updated or in use.	
Index cards	A series of cards that may be arranged alphabetically for the purpose of facilitating references to names, file titles, etc. or numerically for file references.	National Archives
Indexing	The process of establishing access points to facilitate retrieval of records and/or information. (BS ISO 15489-1:2016)	NHS Code of Practice
Information Commissioner Office	The Information Commissioner Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.	ICO
Jointly Held Records	A record held jointly by health and social care professionals, for example in a Mental Health and Social Care Trust. A jointly held record should be retained for the longest period for that type of record, i.e. if social care has a longer retention period than health, the record should be held for the longer period.	NHS Code of Practice
Master Patient Index (MPI)	In medical systems the Master Patient Index (MPI) is an index referencing all patients known to an area, enterprise or Trust. The terms Patient Master Index (PMI) and Master Patient Index are used interchangeably.	NHS Code of Practice
Metadata	Metadata is "data [information] that provides information about other data"	

Word	Definition/Explanation	Source
	It is structured information about a resource. Metadata enables a resource to be found by indicating what the resource is about and how it can be accessed with a series of structured descriptions e.g. for a document: the creator, date, subject and title	
NHS Number	Introduced in 1996, the NHS number is a unique 10 character number assigned to every individual registered with the NHS in England (and Wales). The first nine characters are the identifier and the tenth is a check digit used to confirm the number's validity. Babies born in England and Wales are allocated an NHS number by Maternity Units, at the point of Statutory Birth Notification. The NHS number is used as the common identifier for patients across different NHS Trusts and is a key component in the implementation of the NHS CRS.	NHS Code of Practice
NHS Record	An NHS record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees – including consultants, agency or casual staff.	NHS Code of Practice
Personal Confidential Data (PCD)	Personal Confidential Data is data that contains sufficient information to be able to identify the specific person to whom the data belongs (patient or staff) e.g. name, date of birth, address. This generally excludes publicly available contact lists e.g. staff telephone directories. Note: Previously referred to as Personal Identifiable Data (PID)	
Primary Record	The record that is deemed to be the master record and is therefore subject to the relevant retention schedule. A primary record on a particular record should be either an electronic copy or paper, not both.	
Protective Marking	The process of determining security and privacy restrictions on records. Previously called 'classification'.	NHS Code of Practice
Pseudonymisation	A method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item.	

Word	Definition/Explanation	Source
Publication Scheme	A publication scheme is required of all NHS Trusts under the Freedom of Information Act. It details information which is available to the public now or will be in the future, where it can be obtained from and the format it is or will be available in. Schemes must be approved by the Information Commissioner and reviewed periodically to make sure they are accurate and up to date.	NHS Code of Practice
Record	Information created, received and maintained as evidence and information by an Trust or person, in pursuance of legal obligations, or in the transaction of business. (BS ISO 15489.2016)	NHS Code of Practice
Records System / Record Keeping System	An information system which captures, manages and provides access to records through time. (The National Archives, Records Management: Standards and Guidance – Introduction Standards for the Management of Government Records) Records created by the Trust should be arranged in a record-keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information. Record-keeping systems should contain descriptive and technical documentation to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records, including a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information and to maintain security and confidentiality.	NHS Code of Practice
Referencing	A referencing system helps to provide a means of identifying and retrieving records. Can be used when creating a register or index of records. Several types of referencing can be used: Alphabetical, Numerical, Alphanumeric or Keyword.	National Archives
Register	A list of records, usually in simple sequence such as date and reference number, serving as a finding aid to the records.	National Archives
Registration	Registration is the act of giving a record a unique identifier on its entry into a record-keeping system.	NHS Code of Practice

Word	Definition/Explanation	Source
Retention	The continued storage and maintenance of records for as long as they are required by the creating or holding Trust until their eventual disposal, according to their administrative, legal, financial and historical evaluation.	NHS Code of Practice
Retention Schedule	A schedule containing descriptions of specific record types and the minimum periods that those records should be retained for.	
Review	The examination of records to determine whether they should be destroyed, retained for a further period, transferred to an archival repository.	
Secondary Record	A copy of a primary record held locally for a time specified by that service or department. Only required to be retained for a set period in order to fulfil the requirement of that service or department.	
Storage	The term used when records are likely to require access/retrieval. Storage can be onsite or at the Trust's approved Records Storage and Archiving location.	
Subject Access Request (SAR)	Under the DPA a person can request to see a copy of their records. To do this they must make a subject access request following the process detailed in the Trust's Data Protection Policy.	
Summary Care Records (SCR)	Summary Care Records (SCR) are an electronic record of important patient information, created from GP medical records. It can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.	
Tracking	Creating, capturing and maintaining information about the movement and use of records. (BS ISO 15489-1:2001)	NHS Code of Practice
Transfer of Records	Transfer (custody) – Change of custody, ownership and/or responsibility for records. (BS ISO 15489-1:2001) Transfer (movement) – Moving records from one location to another. (BS ISO 15489-1:2001) Records identified as more appropriately held as archives should be offered to The National Archives, which will make a	NHS Code of Practice

Word	Definition/Explanation	Source
	decision regarding their long-term preservation.	
Version Control	The management of multiple revisions to the same document that enables one version of a document to be identified from another.	National Archives

2.6 Abbreviations

Term / Abbreviation	Definition / description
AHPs	Allied Health Professionals
CQC	Care Quality Commission
DHSC	Department of Health and Social Care
DfE	Department for Education
DPA	Data Protection Act
DSPT	Data Security & Protection Toolkit
ESR	Electronic Staff Record
EPR	Electronic Patient Record
FOI	Freedom of Information
GDPR	General Data Protection Regulation
GMC	General Medical Council
HCPC	Health and Care Professions Council
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IM&T	Information Management and Technology
ISO	International Standards Organisation
JML	Joiner/Mover/Leaver
MCA	Mental Capacity Act
MPI	Master Patient Index
NHS CRS	NHS Care Records Service
NHSLA	NHS Litigation Authority
NMC	Nursing and Midwifery Council
PALS	Patient Advice and Liaison Service
PCD	Personal Confidential Data.

Term / Abbreviation	Definition / description
	Note: Previously referred to as Personal Identifiable Data (PID)
SCHT	Shropshire Community Health NHS Trust

Appendix 3 – Information Asset Owners

3.1 Information Asset Owner responsibilities

The IAO and IAA is responsible for working with others, such as Information Governance, Information, IT, corporate and operational leads, to ensure that we are meeting national requirements as set out in the Data Security and Protection Toolkit (DSPT); and our obligations under the data protection legislation. This includes adhering to Trust policies, developing and implementing processes and procedures and contributing to evidence to demonstrate compliance as part of the annual assessment for the Trust. The key areas of focus include: data quality, records management, know your asset, IT protection, and liaising with suppliers.

Responsibilities include:

- assisting the Information Risk Manager in their duties through providing all appropriate information and support
- ensuring that their staff are aware of their data protection responsibilities
- consulting the Information Risk Manager 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 delegated '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 a 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

There are 10 National Data Guardian standards as set out below:

Standard 1 – Personal confidential data
Standard 2 – Staff responsibilities
Standard 3 – Training
Standard 4 – Managing access
Standard 5 – Process review
Standard 6 – Responding to incidents
Standard 7 – Continuity planning

Standard 8 – Unsupported systems
Standard 9 – IT Protection
Standard 10 – Accountable suppliers

Full guidance can be found here Help (dsptoolkit.nhs.uk)

The above guidance documents will form the foundation for discussion, learning and actions at the IAO and IAA Network groups to ensure that we are pro-actively working towards, contributing to and improving compliance.

Policies that are specifically related to the IAO and IAA roles are:

- Information Risk Policy
- Data Protection Policy (including confidentiality)
- Individual Rights Policy
- Information Security Policy
- Information Quality Assurance
- National Data Opt-Out