South Western Ambulance Service NHS
NHS Foundation Trust

Corporate Records Management Policy

Version:	4.0
Status:	Final
Title of originator/author:	Information Governance Manager
Name of responsible director:	Director of IM&T
Developed/revised by group/committee and Date:	IG Group 26/08/2015
Approved by group/committee and Date:	IG Group 26/08/2015
Effective date of issue: **(1 month after approval date)**	26/09/2015
Next annual review date:	26/09/2018

responsive committed effective

Trust Policy Foreword

South Western Ambulance Service NHS Foundation Trust (SWASFT) has a number of specific corporate responsibilities and obligations relating to patient safety and staff wellbeing. All Trust policies need to appropriately include these.

Health and Safety – SWASFT will, so far as is reasonably practicable, act in accordance with the Health and Safety at Work etc. Act 1974, the Management of Health and Safety at Work Regulations 1999 and associated legislation and approved codes of practice. It will provide and maintain, so far as is reasonable, a working environment for employees which is safe, without risks to health, with adequate facilities and arrangements for health at work. SWASFT employees are expected to observe Trust policy and support the maintenance of a safe and healthy workplace.

Risk Management – SWASFT will maintain good risk management arrangements by all managers and staff by encouraging the active identification of risks, and eliminating those risks or reducing them to the lowest level that is reasonably practicable through appropriate control mechanisms. This is to ensure harm, damage and potential losses are avoided or minimized, and the continuing provision of high quality services to patients, stakeholders, employees and the public. SWASFT employees are expected to support the identification of risk by reporting adverse incidents or near misses through the Trust web-based incident reporting system.

Equality Act 2010 and the Public Sector Equality Duty – SWASFT will act in accordance with the Equality Act 2010, which bans unfair treatment and helps achieve equal opportunities in the workplace. The Equality Duty has three aims, requiring public bodies to have due regard to: eliminating unlawful discrimination, harassment, victimization and any other conduct prohibited by the Act; advancing equality of opportunity between people who share a protected characteristic and people who do not share it; and fostering good relations between people who share a protected characteristic and people who do not share it. SWASFT employees are expected to observe Trust policy and the maintenance of a fair and equitable workplace.

NHS Constitution – SWASFT will adhere to the principles within the NHS Constitution including: the rights to which patients, public and staff are entitled; the pledges which the NHS is committed to uphold; and the duties which public, patients and staff owe to one another to ensure the NHS operates fairly and effectively. SWASFT employees are expected to understand and uphold the duties set out in the Constitution.

Code of Conduct and Conflict of Interest Policy – The Trust Code of Conduct for Staff and its Conflict of Interest and Anti-Bribery policies set out the expectations of the Trust in respect of staff behaviour. SWASFT employees are expected to observe the principles of the Code of Conduct and these policies by declaring any gifts received or potential conflicts of interest in a timely manner, and upholding the Trust zero-tolerance to bribery.

Information Governance – SWASFT recognises that its records and information must managed, handled and protected in accordance with the requirements of the Data Protection Act 1998 and other legislation, not only to serve its business needs, but also to support the provision of highest quality patient care and ensure individual's rights in respect of their personal data are observed. SWASFT employees are expected to respect their contact with personal or sensitive information and protect it in line with Trust policy.

CONTENTS

1 Purpose

1.1 This policy, which is enabled by the Information Governance Strategy, defines how the Trust's corporate records are to be managed throughout their lifecycle from creation or acquisition to disposal.

1.2 Corporate records management supports:

- the day to day business which underpins the delivery of care;
- the knowledge base of the Trust through a history of administrative and managerial decision making;
- legal, regulatory and contractual requirements, including requests for information under the Freedom of Information Act and compliance with the NHS Information Governance Toolkit.

1.3 Information has most value when it is accurate, up to date and accessible when it is needed. Effective records management ensures that information is properly managed and available whenever and wherever there is a justified need for that information, and in whatever media it is required. Therefore the principles of this policy are:

- To ensure information is accessible to those who legitimately need to use it as part of their role
- To ensure information is not duplicated or unnecessarily created because it already exists
- To have a consistent method in how information in similar areas is recorded and referenced
- To hold information for the period it is required and then to destroy it using the appropriate method for that record.

1.4 The Policy will deliver assurance for:

- Confidentiality - the assurance that records are accessed only by authorised people or processes;
- Integrity - the assurance that records are modified only by authorised people or processes and that unauthorised modification attempts will be detected;
- Availability - the assurance that records are available when they are needed.

1.5 The Policy will reinforce compliance with the Trust's Records Retention and Disposal Schedule so that corporate records are retained according to the Schedule and are subject to a final disposal process.

2 Scope

2.1 The policy applies to all corporate records however the retention of records and processes for archiving and destruction applies to both corporate and clinical records

2.2 This policy concerns the lifecycle of a record i.e. from creation to archive or destruction. It does not cover how the information should be disclosed or shared. Guidance on this can be found in the 'Access and Disclosure of Personal and Sensitive Information Policy'

2.3 All staff, volunteers, non-executives and Governors are responsible for abiding by this policy.

3 Definitions

3.1 The table below lists and describes the words and terms which have specific meaning in the context of the policy.

Term	Explanation
Record	A record is evidence or a collection of evidence relating to a period of time, an event or series of events and of how decisions were made. A record may be in any format (physical, electronic or a combination) and can be a document, spread sheet, photograph, audio recording or any combination. Records are generally permanent but can be amended in some circumstances.
Corporate Information	This is information generated and received by the Trust other than clinical/care (or service user) information. The term describes the records generated by an organisation's business activities, and therefore will include for example records relating to personnel, estates, finance, information management & technology, administration, purchasing and supplies.
Personal Data	Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes items of information such as an individual's name, address, age, race, religion, gender and physical, mental or sexual health.
Sensitive Data	This is information, which if disclosed to unauthorised persons could: i. adversely affect the reputation of the Trust or its staff or cause substantial distress to individuals ii. make it more difficult to maintain the operational effectiveness of the Trust iii. cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations iv. prejudice an investigation, or facilitate the commission of crime or other illegal activity v. breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies vi. breach statutory restrictions on disclosure of information vii. disadvantage the Trust in commercial or policy negotiations with others or undermine the proper management of the Trust and its operations
Senior Information Risk Officer (SIRO)	A board level individual who understands how the business of the Trust will be impacted by information risks and will ensure that any such risks are identified and managed. An organisation has one SIRO.

Term	Explanation
Information Asset Owner (IAO)	The officer within SWAST responsible for the management of an information asset. The asset could be an electronic system e.g. C3, or a key set of documents e.g. paper p-files. All information assets are listed within the Information Asset Register which is administered by the Information Governance Manager.
NHS Number	A unique identifier introduced in 1996. The objective is for all individuals registered with the NHS in England and Wales to have an NHS Number. Whilst this policy is concerned with corporate records, some records may consist of both corporate and clinical records. The NHS Number is almost certain to be present on clinical records and may be used as a link between corporate and clinical records or used as part of the record identifier.
Retention Period	The minimum period for which a record must be kept. This may be determined by law, regulatory requirements or NHS guidance.
Confidentiality	The assurance that information is accessed only by authorised people or processes.
Integrity	The assurance that information is modified only by authorised processes or that unauthorised modification will be detected.
Availability	The assurance that information will be available when it is needed.

4 Duties, Responsibilities, Governance and Reporting

4.1 Duties & Responsibilities

Role	Duties and Responsibilities
Chief Executive	The Chief Executive has overall responsibility, on behalf of the Trust Board, for ensuring the implementation of this policy.
SIRO	The Senior Information Risk Officer is responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and champions information security risk management at Board level.
Caldicott Guardian	The Caldicott Guardian is responsible for ensuring patient information is handled in accordance with the Caldicott requirements. Although this policy deals with corporate information, there are likely to be scenarios where both patient and corporate information are processed side by side.
Executive Directors	Executive Directors are responsible for:- a) implementing this policy on behalf of the Chief Executive b) delegating responsibility to managers for the policy's implementation c) monitoring the effectiveness of managers in implementing the policy d) ensuring sufficient resources are available to deal with the implementation of this policy
Non-executive Directors.	The Chairman and Non-executive Directors have assurance responsibilities for the Information Governance agenda, in particular at Board level and through the Quality and Governance Committee.
Information Governance Manager	The IG Manager is responsible for co-ordinating the Trust's corporate records management activities and managing the IG Team to support implementing the policy.

Role	Duties and Responsibilities
Information Asset Owners & Managers	Information Asset Owners & Managers should:- a) be aware of their responsibilities under this policy b) document activities in respect of records management for their function c) ensure appropriate system specific training is provided to users d) assist in the completion of corporate records audits for their function.
All staff	All staff should:- a) be responsible for the records they create or use in the performance of their duties b) familiarising themselves and complying with this policy.

4.2 Governance & Reporting

a) The implementation and monitoring of this policy will be overseen by the Information Governance (IG) group. They will:

- assist in identifying actions required to implement this policy and ensure they are included within the IG work programme
- approve the records audit process and timetable of implementation
- monitor actions arising from the records audit

b) Actions arising from the implementation of this policy will be incorporated into the IG work programme. The work programme is developed by the IG Group and progress updates are submitted to Directors, the Quality & Governance Committee and the Board according to the Trust's schedule of meetings.

5 Risk Assessment

5.1 The Information Governance Manager will evaluate the risk of non-compliance with this policy in accordance with the Trust's Risk Management Strategy.

5.2 Any risks identified during the risk evaluation process that cannot adequately be controlled will be forwarded to the holder of the directorate risk register (for risks scoring less than 10) or the Risk Manager (for risks scoring 10 or more).

5.3 Where a set or collection of records has been approved by the IG Group for inclusion in the Information Asset Register (see the Information Asset Management Policy for details), the Asset Owner will be required to carry out information risk assessments to manage the Confidentiality, Integrity and Availability of the asset according to its business criticality and value.

6 Relevant Legislation and Guidance

6.1 The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice and other relevant legislation and codes, in particular:

- The Public Records Act 1958
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

7 Record Creation and Naming

7.1 Records created must 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. The record itself must also contain key information for future reference.

7.2 Each function (for example, Finance, Estates, IT) must document its activities in respect of records management. This must take into account any legislative and regulatory environment in which it operates. The documentation must contain sufficient description to enable the system to be operated efficiently and the records held in the system to be understood. This will include:

a) Naming convention for records created or received. This must ensure:

i. each record has a unique name

ii. the name is meaningful and closely reflect the records contents

iii. expresses elements of the name in a structured and predictable order

iv. locates the most specific information at the beginning of the name and the most general at the end

v. gives a similar structured and worded name to records which are linked

vi. Elements of a file name could include:

- A reference number so records relating to the same issue can be found e.g. employee number, invoice number, NHS Number etc
- Version control number
- The date the record is created or received
- Who created the record

b) Information to be included within the record itself. Any hard copy records received must be date stamped. Other information that needs to be recorded will vary considerably depending upon the type of record, but could include elements listed in vi) above, plus the location of where the record is held. Templates for key documents such as policies already prompt the author to include certain information. Although this policy is not concerned with clinical records, there may be situations where it is beneficial to also record the patient's NHS Number to assist with the accurate processing of that information e.g. a patient's complaint.

c) The file structure used to store the information, to include electronic file share, shared email accounts and hard copy indexing and filing systems. Where mixed media are used to store information, the same file structure for each media type should be used if possible.

d) User guidance on any system involving records management to ensure information is recorded as intended. As a minimum this must cover:

i. what information is recorded, how and why

ii. how to validate information against other records if appropriate

iii. how to identify and correct errors

iv. how the information will be used

v. how to update information and add in information from other sources

e) Completion of the Trust's records register (managed by the Information Governance team) with the record sets held and owned by that function. This will help to identify:

i. who holds various records sets

ii. who holds the originals of documents and owns the record sets

iii. how they are stored and if there are adequate storage facilities

iv. if they contain any personal or sensitive information

v. who needs to access the records

vi. any security needed to ensure there is no unauthorised access to the records.

vii. How long the records should be kept for

8 Classification of Records

8.1 NHS England's Document and Records Management Policy v 3.0 (Page 24) contains guidance on their adoption of the Government Security Classifications which were introduced on 02/04/2014 (http://www.england.nhs.uk/wp-content/uploads/2014/02/rec-man-pol.pdf).

8.2 There is no current Trust policy on classification or protective marking.

9 Filing and Storing of Records

9.1 Each function must document the filing structure to be used, as described in section 7 of this policy and store records accordingly.

9.2 The long term storage of emails in Outlook should be avoided, especially those with attachments due to the impact these have on storage volumes and retention schedules which may lead to a breach of the Data Protection Act. Emails that need to be kept should be stored on the network file share with other relevant documents, or deleted if they are not required.

9.3 The Trust has systems in place to back up information stored on the network drive. Therefore it is important that any records stored on the hard drive of any mobile device should be moved / copied to the network drive to ensure they are backed up. Personal data should never be stored on a mobile device.

9.4 Storing information on network drives, the intranet and internet enables people across the large geographic area of the Trust to access that information. Publishing information on the intranet and/or internet also eliminates the need for multiple copies of the document to be stored and for people to access the most up to date version of that document. Publication of documents in this way is encouraged where it is appropriate.

9.5 As an alternative to keeping paper records, scanned copies may be an option. This would also increase the accessibility of the information across the Trust if required.

When scanning documents, consider:

- The cost associated with the initial scan and any later media conversion, especially if the record has to be kept for a long period of time.
- If any legislation requires that the original document must be kept and/or submitted as evidence in court.

9.6 Records can be stored on a wide range of media and systems. Ensure that the information is still available as technology evolves and systems change.

10 Record Tracking

10.1 For hard copy records, e.g. personnel files, ensure a system exists to log when the record has been released and to whom. A chase system may also be required to ensure the record is returned.

10.2 It may also be necessary to track a record to support a consultation and/or approval process. This could be logged either in a separate document/system, within the document itself or by keeping a copy of an email.

11 Retention of Records

11.1 The Trust has to keep records for predetermined periods of time for legislative, regulatory and general business purposes. A Trust-wide Records Retention Schedule has been compiled, based on the NHS national schedule and can be found in the Information Governance pages on the intranet and offers more comprehensive guidance.

11.2 Records must be kept for the minimum period stated in the Retention Schedule. The Information Governance Group will approve any amendments to the records retention schedule.

11.3 Records should not ordinarily be kept for longer than 30 years. The Public Records Act 1958 does, however, provide for records, which are still in current use to be legally retained for longer provided prior approval is obtained as referred to in 11.5 below. Additionally, separate legislation may require the retention of records for longer than 30 years (e.g. Control of Substances Hazardous to Health Regulations)

11.4 The minimum retention periods should be calculated from the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2004 and the last in September 2007, and for which the retention period is seven years, should be kept in its entirety at least until the beginning of 2015.

11.5 The Trust must not keep records for a shorter retention period than the minimum set out in this schedule, but there may be circumstances in which they need to apply a longer retention period. Any decision to extend must ensure that the retention period does not exceed 30 years unless prior approval has been obtained via The National Archives.

11.6 In respect of any records that contain personal data as defined by the Data Protection Act 1998, consideration should be given to the fifth principle of the Act, i.e. that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

11.7 Managing records according to the Retention Schedule will:

- Maintain compliance with Principle 5 of the Data Protection Act 1998 (personal data should not be kept longer than is necessary);
- Reduce Freedom of Information administration as records must be supplied to a requestor if they are held, even if they are outside their retention period;
- Reduce the costs and space associated with storing records unnecessarily.

11.8 Once records have reached their (extended) retention period they must be subject to a final disposal which will be irreversible destruction or a permanent archive for records of historic(al) interest.

11.9 Where a set of records contains records with differing retention periods and they cannot be separated without compromising the context and meaning of the set, the set will be retained for the longest of the individual retention periods.

11.10 The Information Governance Team arranges the archiving and destruction of physical records and the ICT Service Desk can offer advice on the secure destruction of electronic records, computer hard disks, CD/DVD.

12 Processes for Archiving and Destruction

12.1 All staff are responsible for regularly reviewing the information that they hold and for ensuring that they do not retain information that is no longer required. This might take the form of, for example, reviewing emails and deleting any that are no longer required or sorting through and disposing of paper documents on desks.

12.2 Toward the end of the relevant minimum retention period for a record, the record's owner should review the record and decide on the next steps. One of the following actions will usually apply:

a) **Review**: records may need to be kept for longer than the minimum retention period due to on-going administrative need. As part of the review, staff in the Trust should have regard to the fifth principle of the Data Protection Act 1998, which requires that personal data is not kept longer than is necessary. If it is decided that the records should be retained for a period longer than the minimum the Trust's Records Retention Schedule may need to be amended.

b) **Archive**: Some paper records may need to be kept for a significant period of time but are no longer current (i.e. you are unlikely to need them on a regular basis). These should be archived using "SOP – Archiving and Confidential Waste Destruction". The IG Team will contact the archived paper record's owner when the record is due for destruction to discuss whether the record should be kept or destroyed. If you need to archive electronic files relating to corporate records please contact the Information Governance team for advice.
Destroy: Some paper records do not need to be kept but do contain personal or sensitive information. These should be destroyed securely either by shredding using an appropriate machine (*at least security Level 3 as defined by DIN32757*) or destroyed using the disposal process within "SOP – Archiving and Confidential Waste Destruction". The document also sets out the process to destroy archived records once they are no longer required

12.3 As referred to in section 9.2, the long term storage of emails should be on the file share network rather than within Outlook. Regular reviews of files kept should be undertaken to ensure unnecessary information is not being stored.

12.4 For the destruction of electronic records this is detailed in the IMT Security Policy and advice should be sought from the ICT Services Department.

13 Digital Continuity

13.1 The Information Asset Management Policy gives more comprehensive guidance but digital continuity is the assurance that digital information is available for as long as it is required. Access to digital information must survive operating system upgrades, application software upgrades, organisational mergers, system decommissioning etc.

13.2 Information Asset Owners are responsible for ensuring they have Digital Continuity plans for relevant records.

14 Training Requirements

14.1 Line Managers are responsible for ensuring their staff complete the relevant training available through the Information Governance Training Programme.

14.2 Additional records management training and guidance on the use of Trust systems will be provided for users by Information Asset Owners to ensure that they are competent to carry out their designated duties. Where identified, further specialist records management training will be included within the Information Governance Training Programme.

14.3 More tailored and focussed training may be sourced from providers such as the National Archives and the Institute of Health Records and Information Management.

15 Monitoring

15.1 To ensure corporate records management is effective within the Trust and comply with prevailing IG Toolkit requirements, a minimum of four corporate records audits will be completed each year. The Information Governance Group approves the audit process and the Directors' Meeting approves the selection of business areas to be audited. The objectives of the audit will be:

- To ensure record keeping systems are documented, fit for purpose and effective
- To identify areas requiring development or improvement
- To determine if the NHS Number needs to be included in any records

15.2 Actions for improvement identified from the audits and actions needed to implement this policy will be monitored by the IG Group. The group will also regularly review adverse incidents relating to all aspects of IG, including corporate records management, to identify if any further actions / changes are required.

15.3 The IG Toolkit includes requirements relating to corporate records management. Compliance against these requirements and actions to deliver them will be included within the IG work programme.

16 Associated Documents

16.1 SWAST

- Information Governance Strategy
- Keeping Information Private and Confidential - A Guide for Staff
- SOP – Archiving and Confidential Waste Destruction
- Records Retention Schedule
- Records Register
- Clinical Records Management Policy
- Risk Management Strategy
- SOP – IG05 – Information Risk Assessments

16.2 External to SWAST

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- Records Management: NHS Code of Practice;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;
- The NHS Information Governance Toolkit.

Appendix A

Version Control Sheet

Version	Date	Author	Summary of Changes
1.0	23/03/12	Mary Bartlett	First draft of new policy based upon existing guidance issued to staff and national policy.
1.1	26/03/12	Mary Bartlett	Amendments to Duties and Responsibilities requested by Francis Gillen.
2.0	08/01/13	Kate Minett	Amending headings and content order to comply with Framework for Policy Development. Addition of section 6 regarding legal/regulatory framework. Addition of section regarding proposed changes to security classification levels. Additions to section 10 regarding record retention and addition of section regarding archiving/destruction processes.
2.1	14/01/13	Kate Minett	Further amendments to sections 11, 12 and 13 following discussion with Mary Bartlett. Adding link to HMG Security Policy Framework at 8.6.
2.1	16/01/13		Submitted to Information Governance Group
2.2	01/03/13	Kate Minett	Updating formatting to match new template.
3.0	01/06/14	Debbie Bridge	Scheduled review of Policy and inclusion of New Government Security Classification Information Section 4.5 – Information Governance Manager responsibilities amended. Section 4.6 - Records Manager responsibilities added, some responsibilities previously attributed to IG Manager now being covered by Records Manager Section 7 - Information relating to new Government classification scheme included. Section 15.1 Removal of Risk Management Process this is incorporated within Risk Management Strategy 14.1 Links updated where appropriate
3.1	12/06/14	Debbie Bridge	Feedback from IG Group. Section 11.4 - Inclusion of Electronic Record Destruction
3.4	20/07/2015	Debbie Bridge Information Governance Manager	Throughout document references to Records Manager post removed, post is no longer current. 1.1 Updated in line with current practice

Version	Date	Author	Summary of Changes
			1.2 Inclusion of supporting information 1.4 Inclusion of CIA assurance 1.5 Inclusion of records retention reference 2.1 Updated in line with current practice 3.0 Definitions replaced with Table Format 3.1 Inclusion of SIRO 3.1 Inclusion of Records Retention 4.0 Duties and Responsibilities replaced with table format 4.2 Governance section replaced with Governance and Reporting section updated in line with current practice 5.0 Section amended to reflect current practice in consultation with Risk Manager 6 Inclusion of separate Legislation & Guidance Section 8 Classification of Records all references to obsolete classification systems removed Inclusion of link to NHS Document and Records Management Policy 9 Removed reference to records register as not complete for all areas 11 Updated in line with current practice 12.2 Archive of Electronic Records amended to advice as no process currently defined 13 New section relating to Digital Continuity 16 Previous Sections 14 & 15 amalgamated