Maidstone and Tunbridge Wells
NHS Trust

Ref: FOI/GS/ID 4374

Please reply to:
FOI Administrator
Trust Management
Maidstone Hospital
Hermitage Lane
Maidstone
Kent
ME16 9QQ
Email: mtw-tr.foiadmin@nhs.net

30 November 2017

Freedom of Information Act 2000

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to medical devices cyber security.

1. Please State how many networked diagnostic medical imaging devices, e.g. CT, ultrasound, etc. are used by the Trust? Please include all DICOM endpoints that have a local image store when calculating this. I.e. include diagnostic workstations as well as scanners.
2. How many of these devices are full drive encrypted or have their image store encrypted or do not have a local image store?
3. Please state how many of these devices have operating system and application patches applied and the frequency. Below table should be used
4. Please state number of devices connected to the trust network in below table.
5. How many of these devices have anti-virus or other anti-malware software that is updated, when new definitions/updates are available?
6. The next question relates to dataflows. For the definition of this question a dataflow can be viewed as either a DICOM send or a DICOM Query Retrieve. So for example if a capture device can send a study to a workstation and the same workstation is allowed to Query and Retrieve a study from the same capture device this would be counted as 1. Please complete table with number of data flows.
7. Do you have policy and procedure for secure removal of patient data on loan, lease, trial or end of service devices that includes medical devices?
8. Do you have a Legacy I.T. Hardware & Software Security Policy?

1. 295 Medical Imaging Devices
2-6. The trust has applied Section 31 (1)(a) of the FOI Act (Law Enforcement) to these questions as providing this information could compromise the security of the Trust's network / data and might materially cover activity which forms part of ongoing criminal investigations

The information which has been withheld is exempt from disclosure under section 31(1)(a) of the Freedom of Information Act. The relevant parts of the ICO guidance on the subject (https://ico.org.uk/media/for-

organisations/documents/1207/law-enforcement-foi-section-31.pdf) run as follows:
31.—(1) Information is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime. It could be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures. It is the view of this trust's Information security function that disclosure of the information above would prejudice our ability to resist cyber-attacks, etc. on our systems.

7. & 8.

The following policy and procedure covers all devices.

MAIDSTONE AND TUNBRIDGE WELLS NHS TRUST

Information Lifecycle Management Policy and Procedure

Target audience:	All Trust staff
Main author:	Head of Information Governance **Contact details: 01892 634029**
Other contributors:	Director of Health Informatics
Executive lead:	Chief Nurse (Senior Information Risk Owner)
Directorate:	Health Informatics
Specialty:	Information Governance
Supersedes:	Data Quality Policy and Procedure [RWF-OPPCS-NC-TM40] Records Management Policy and Procedure [RWF-OPPCS-NC-TM1] Information Security Incident Report [RWF-OPPCS-NC-TM10]
Approved by:	Information Governance Committee, 24th November 2016
Ratified by:	Policy Ratification Committee, 13th December 2016
Review date:	December 2019

Disclaimer: Printed copies of this document may not be the most recent version.
The master copy is held on Q-Pulse Document Management System
This copy – REV1.0

Document history

Requirement for document:	• To set out the framework for effective information and record management within the Trust, commensurate with legal, professional, operational and information needs.
Cross references (external):	1. Public Records Act 1958 2. Data Protection Act 1998 3. Access to Health Records Act 1990 4. Freedom of Information Act 2000 5. The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 6. Environmental Information Regulations 2004 7. The Common Law Duty of Confidentiality 8. The NHS Confidentiality Code of Practice 9. The NHS Care Records Guarantee 10. NHS Records Management Code of Practice 11. Government Security Classifications 2014 12. Information Governance Toolkit 13. The NHS Information Quality Assurance Programme 14. Care Quality Commission Records Management Standards 15. ISO accreditation standards
Associated documents (internal):	• Data Protection Policy [RWF-OPPCS-NC-TM5] • Health Records Policy and associated Standard Operating Procedures [RWF-OPPCS-NC-TM31] • Freedom of Information Act 2000 Policy [RWF-OPPCS-NC-TM2] • ICT Acceptable Use Policy and Procedure [RWF-OPPCS-NC-TM8] • Email Policy and Procedure [RWF-OPPCS-NC-TM6] • Security Policy and Procedure [RWF-OPPCS-NC-FH3] • Locating Missing Case Notes and Missing Case Note Audit Trail [RWF-OPPM-CORP28]

Keywords:	Record	Retention	Data Quality
	Tracking	Archive	Marking
	Disposal	Disclosure	Safe Transfer
	Police	ICT Acceptable Use	Information Lifecycle
	Information Management		

Version control:		
Issue:	**Description of changes:**	**Date:**
1.0	New policy and procedure consolidating the following documents: Data Quality Policy and Procedure [RWF-OPPCS-NC-TM40] Records Management Policy and Procedure [RWF-OPPCS-NC-TM1] Information Security Incident Report [RWF-OPPCS-NC-TM10]	December 2016

Policy statement for

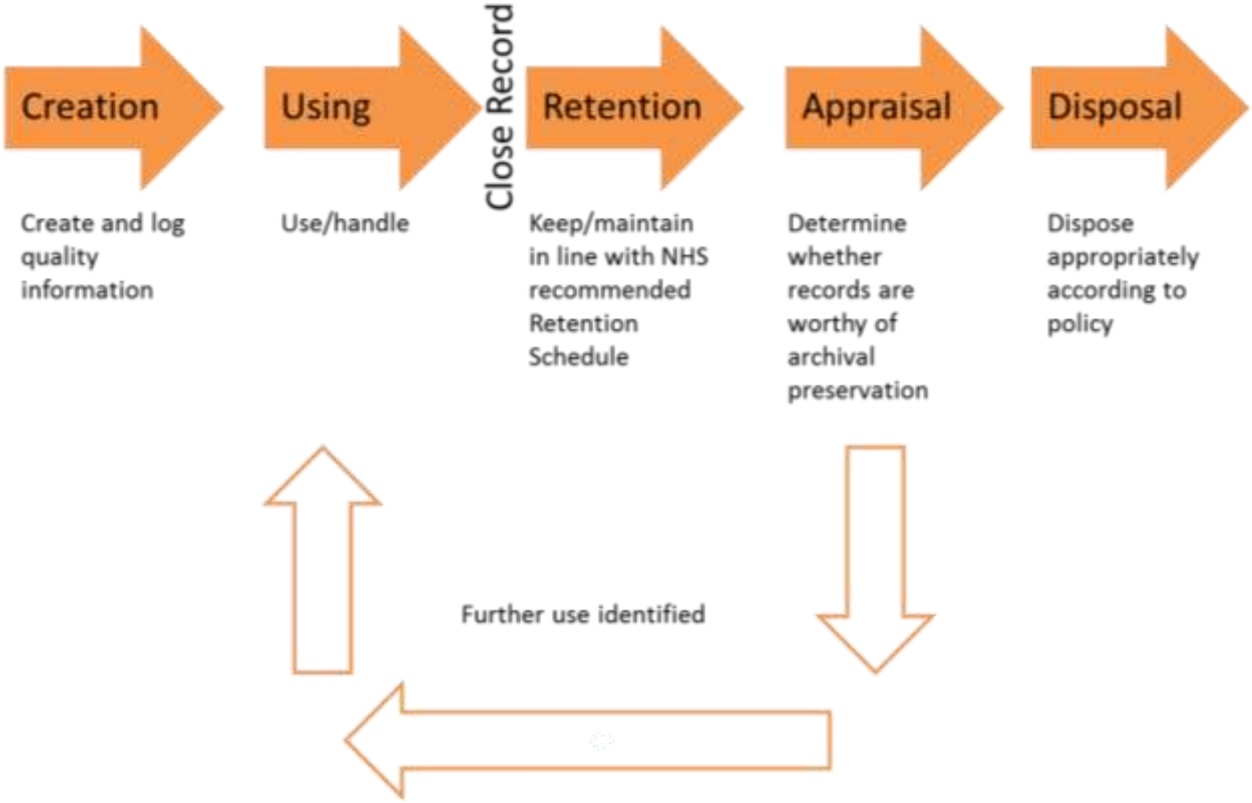
Information Lifecycle Management

The purpose of this document is to set out duties which apply and the standards to be adopted within the Trust to provide a robust Information Lifecycle (also known as Records Management) framework for the current and future management of information.

Within this framework the Trust is developing specific guidance and procedures to ensure that its records, whether paper or electronic, clinical or non-clinical, are managed and controlled effectively, are of the highest quality and at best value, commensurate with the organisation’s legal, operational and information needs.

Table of Contents

Diagram of Information Lifecycle


Creation
Create and log quality information
Using
Use/handle
Close Record
Retention
Keep/maintain in line with NHS recommended Retention Schedule
Appraisal
Determine whether records are worthy of archival preservation
Disposal
Dispose appropriately according to policy
Further use identified

1.0 Introduction and scope

- Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958. The Act requires that all public bodies have effective management systems in place to deliver their functions.
- The primary reason, for health and social care, for managing information and records is for the provision of high quality care.
- Section 46 of the Freedom of Information Act 2000 required organisations covered by the Act to have records management systems which will help then perform their statutory function.
- Organisations may be asked for evidence to demonstrate they operate a satisfactory records management regime
- The Trust's records are its corporate memory, providing evidence of actions and decisions and a vital asset to support daily functions and operations.
- Trust records should be accurate and complete, in order to facilitate audit, fulfil the Trust's responsibilities and protect its legal and other rights. Records should show proof of their validity and authenticity so that any evidence derived from them is clearly credible and authoritative.
- Records support policy development and managerial decision making, protect the interests of the Trust and the rights of patients, staff and members of the public.
- Records support consistency, continuity, efficiency and productivity and help us deliver services in consistent and equitable ways.
- The policy covers information regardless of the media/format in which it is held and the content of such information i.e., it applies to information held on paper and/or in other physical forms such as electronic, microfilm, negatives, photographs, audio or video recordings.
- The key components of records management are:
    - Record creation
    - Record keeping
    - Record maintenance (including tracking or record movements)
    - Access and disclosure
    - Closure and transfer
    - Appraisal
    - Archiving
    - Disposal
- Collectively these components are known as the 'information lifecycle'.
- Implementation of the policy will ensure that:
    - Records are available when needed
    - Records can be accessed – records and the information within them can be located and displayed in a consistent way and that the current version is identified where multiple versions exist

    - 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.
- Not all documents are records. Documents are created by and when planning what needs to be done. Records are created when something is done. Documents can change. Records must not be altered once completed.
- Record keeping systems should be easy to understand, clear and efficient in terms of minimising staff time and optimising the use of storage space.
- Access is a key part of any records management process. Fast, efficient access to records unlocks the information and knowledge they contain.
- This policy applies to anyone creating or using information for or on behalf of the Trust including, but not limited to, employees formally employed by the Trust, those employed by the Trust on an honorary contract, volunteers, contractors, students, locum and agency staff.

2.0 Definitions / glossary

Archive	Those records that are appraised as having permanent value for evidence of on-going rights or obligations, for historical or statistical research or as part of the corporate memory of the organisation. - (The National Archives, Records Management Standard 3.1). It is a legal requirement for NHS records selected as archives, to be held in a repository approved by The National Archives.
Authenticity	An authentic record is one that can be proved: • To be what it purports to be; • To have been created, or sent, by the person purported to have created or sent it; and • To have been created or sent at the time purported. (BS ISO 15489-1:2001 E) – To ensure the authenticity of records, organisation should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record

	creators are authorised and identifiable and that records are protected against unauthorised addition, deletion, alteration, use and concealment.
Breach of confidentiality	The unauthorised disclosure of personal information provided in confidence.

Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing
Confidential information	Confidential information is information provided in confidence. This can relate to patients, staff or any other information (such as contracts, tenders, etc.) held in any form (such as paper, electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer devices such as PCs, laptops, iPads, mobile phones) or even passed by word of mouth
Corporate records	Records (other than health records) that are, or relate to, the Trust’s business activities, covering all the functions, processes, activities and transactions of the Trust and its employees.
Current records	Records necessary for conducting the current and on-going business of the Trust.
Data Protection Officer	A designated person within an organisation who is responsible for making sure that the organisation follows the Data Protection regulations.
Destruction	The process of eliminating or deleting records beyond any possible reconstruction (BS ISO 15489-1:2001 E)
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.
File	A file is usually the basic unit within a records series.
File referencing system	A plan for organising records so that they can be found when needed (the National Archives, Records Management Standard 1.1)
Folder	An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction.
Health record	(The Data Protection Act 1998 S68(2)) A record consisting of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.
Information	An information asset is a body of information, defined and

asset	managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

Information asset register	A list of personal and non-personal Information Assets held by the Trust
Information lifecycle	The series of stages through which information passes from creation and initial storage to the time when it becomes obsolete and is deleted.
Information provided in confidence	Information that has been given with an expectation that it is not going to be widely disclosed.
Integrity of records	Refers to a record being complete and unaltered. It is necessary that a record be protected against unauthorised alteration. Any unauthorised annotation, addition or deletion to a record should be explicitly identifiable and traceable.
Metadata	"Data that provides information about other data". Metadata summarizes basic information about data, which can make finding and working with particular data easier.
Patient identifiable information	Anything that may be used to identify a patient directly or indirectly. For example: • Name, address, post code, date of birth; • Pictures, photographs, videos, audio-tapes or other images of patients; • NHS Number and local patient identification codes; • Rare diseases, drug treatments or statistical analyses which have very small numbers within a small population.
Person identifiable information	Anything that contains the means to identify an individual.
Public records	Records as defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives. Records of NHS organisations (and those of predecessor bodies to NHS organisations) are defined as public records under the terms of the Public Records Act 1958 Sections 3(1), 3(2). NHS records may not be retained for longer than 20 years without formal approval by National Archives.

Record	Information being created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Examples include: • Patient health records (electronic or paper based); • Records of private patients seen on NHS premises; • Accident and Emergency, birth and all other registers; • Corporate/Administrative records (e.g., personnel, estates, financial and accounting records, notes associated with complaint handling etc.); • X-ray and imaging reports, photographs and other images; • Websites and intranet sites that provide key information to patients and staff; • Text messages and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype; • Microform (e.g., fiche/film); • Audio and video tapes, CCTV footage, CD-ROM, DVD, etc. • Computer databases, output, portable storage media and all other electronic records; • Emails; and • Material intended for short term or transitory use, including notes and ‘spare’ copies of documents. This list is not exhaustive.
Senior Information Risk Owner	The senior person responsible for dealing with information risk in the Trust.

3.0 Duties

Senior Information Risk Owner

The Chief Nurse as Senior Information Risk Owner (SIRO) is responsible for:

- Ensuring the development, implementation and review of Information Governance policies
- Ensuring the Board is adequately briefed on Information Governance issues.

Caldicott Guardian

The Medical Director as Caldicott Guardian is responsible for:

- Ensuring records containing patient identifiable information are managed in an appropriate and secure manner in accordance with the NHS Caldicott principles.

Data Protection Officer

The Director of Health Informatics as the Data Protection Officer and Information Governance Lead is responsible for:

- Taking the strategic lead on records management and ensuring that records are managed in accordance with the Department of Health Records Management Code of Practice and the Data Protection Act 1998.
- The Trust senior manager responsible for data quality.

Information Governance Committee

The Information Governance Committee is accountable to the Trust Management Executive (TME) and responsible for ensuring that this policy is implemented and that information and records management systems and processes are developed, co-ordinated and monitored to provide assurance to the Trust Board in this respect.

Data Quality Steering Group

The Data Quality Steering Group has delegated responsibility for Data Quality and is responsible for providing assurance to the Information Governance Committee in this respect and is accountable to the Informatics Steering Group.

Head of Information Governance

The Head of Information Governance is responsible for advising on the development of policy and guidance and also for providing operational support related to Information Governance to the Trust.

Health Records Manager

The Health Records Manager is responsible for the development and maintenance of health records management policies and practices throughout the Trust, in particular for drawing up guidance for good health records management and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

Information Asset Owners (IAO)

The overall responsibility for local information/records management is devolved to the relevant directorate and department managers. As Information Asset Owners they have to ensure that the information assets controlled within their operational unit are managed in a way which meets the aims of this policy and its associated procedures. The IAOs have to:

- Maintain a local Information Asset Register;
- Conduct regular records management audits. Examples of an audit planning document; Checklists to measure/test compliance for key components of records management; & an audit outcome report are attached at Appendix 4;

- Identify all information/records which are integral to the continuing functioning of the activities of the Trust;
- Review information/record management processes for the entire lifecycle from creation through to permanent preservation or destruction;
- Develop adequate audit trails to track use and location of records;
- Review storage accommodation for active paper records to ensure that they are secure from fire, flood and theft;
- Review risks to their information assets, prioritise and maintain oversight of actions agreed to mitigate such risks;
- Establish access controls so that only those who need to know can access the records;
- Ensure users share records and the information they contain in accordance with the Data Protection Act 1998 and Caldicott Principles;
- Define best practice guidelines for keeping, holding, storing and disposing of records in line with national and local guidance;
- Promote local and national guidelines by facilitating training for all grades of staff;
- Liaise with other local records managers within the Trust to ensure a coherent approach to the management of information/records of the same or similar nature;
- Monitor staff performance through quality control and internal audits and identify particular training needs;
- Ensure inclusion of essential information/records management issues/practices and information incident reporting in the induction training for all new staff;
- Ensure that records management issues are considered when planning or implementing ICT systems, when extending staff access to new technologies and during re-structuring or major changes to their area of responsibility.
- Support the Trust SIRO and Information Governance Committee in maintaining awareness of the risks to their information assets.

Information Asset Administrators (IAA)

Information Asset Administrators are the operational staff responsible for the day to day control and use of one or more information assets, in particular they:

- Ensure that policies and procedures are followed:
- Recognise actual or potential security incidents;
- Consult their Information Asset Owner on incident management; and
- Ensure the Information Asset Registers are accurate and up to date.

All staff

It is the responsibility of all staff to adhere to the principles set out in this document and any related policy/procedure to help maintain the availability, effectiveness, security and confidentiality of information.

There are a number of record keeping codes that people associated with certain professional bodies must adhere to as part of their profession.

4.0 Training / competency requirements

All Trust staff will be made aware of their responsibilities for record keeping and record management through mandatory annual information governance training.

Where errors in data quality are consistently found users will be offered additional training, to be delivered by the Clinical Applications Support and Training Team.

5.0 Procedure

All records will be part of an Information Asset, typically a collection of associated records, with a designated Information Asset Owner, and will be recorded as such on an Information Asset Register (which is held centrally by the Head of Information Governance).

All records must be kept securely with a level of security appropriate to their sensitivity to prevent unauthorised or unlawful access and to ensure against accidental loss, damage to or destruction of the records.

The following key principles should be applied to all types of record:

- Records should be factual, consistent, accurate and up to date
- Records should be recorded during an event or as soon as practicable thereafter. Where data is omitted in order to avoid delaying patient care, the user will note that omission and return to complete the record as soon as possible.
- Entries should be clear and legible
- Where appropriate entries should be dated, timed and if required signed.
- Records should be stored consecutively (place data in a logical order) – particularly for paper records
- Records should be kept in the appropriate file or folder to guard against loss.
- Clinical records should conform to the Royal College of Physicians Standards for the clinical structure and content of patient records.
- Where codes are used these will comply with national standards or directly map to national standards.
- The NHS Number will be used as the patient primary identifier.
- Patient data will be regularly assessed for accuracy by undertaking various validation checks.

The Trust adopts the Government Security Classifications published in April 2014 for its records. All information used by the Trust is by definition ‘Official’.

Trust records do not, routinely, need to be protectively marked with their classification. Marking should, however, be applied for personal confidential data and commercially sensitive information when any records are leaving the Trust. This applies to both paper and electronic documents/records. The appropriate classifications and markings are:

OFFICIAL – SENSITIVE: PERSONAL and OFFICIAL – SENSITIVE: COMMERCIAL

If in doubt the appropriate Information Asset Owner should be consulted.

Further guidance relating to the Protective Marking Scheme is available at Appendix 5.

The following paragraphs map the five phases of the information lifecycle (Creation, Use, Retention, Appraisal and Disposal) and explain how information that is being, will be or has been created for or on behalf of the Trust has to be managed.

5.1 Creation

When creating information in the first instance, the following should be adhered to, the information must be:

- Available when needed – to enable a reconstruction of activities or events that have taken place;
- Accessible to all members of staff that require access in order to enable them to carry out their day to day work – the information must be located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist;
- Interpretable, clear and concise – the context of the information must be clear and be able to be interpreted appropriately i.e., who created or added to the record and when, during which business process and how the record is related to other records;
- Trusted, accurate and relevant – the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant;
- Secure – The information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required/retained;

5.1.1 Scanning

For reasons of business efficiency, or in order to address problems with storage, consideration should be given to the option of scanning into electronic format, records which currently exist in paper format. Where this is proposed, the factors to be taken into account include:

- The costs of the initial and then any later media conversation to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;

- o The need to consult, in advance, with the local Place of Deposit, or The National Archives, with regard to records which may have archival value, as the value may include the format in which it was created; and
- o The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular standard BS 10008 – Electronic Information Management – Ensuring the authenticity and integrity of electronic information.

Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original. A scan of not less than 300 dots per inch or 118 dots per centimetre as a minimum is required.

Methods to ensure that scanned records can be considered authentic are:

- A written procedure outlining the process to scan, quality check and destruction process for the paper record;
- Evidence that the process has been followed;
- An audit trail that can show that no alterations have been made to the record after the point they have been digitised;
- Fix the scan into a file format that cannot be easily edited such as Portable Document Format (PDF).

Common errors include:

- Only scanning one side and not both sides, including blank pages;
- Scanning a copy of a copy leading to a degraded image;
- Not using a method that can show that the scanned record has not been altered after it has been scanned;
- Not having a long term plan to enable the digitised records to be stored or accessed over the period of their retention.

When creating information you should consider:

- What information is being recorded and how it should be recorded;
- Why the information is being recorded;
- How the information will be validated (with patients or carers or against other records) to ensure that the correct data is being recorded;
- How to identify and correct errors and how to report errors if they are found;
- The use of the information, what the record will be used for and why the timeliness, accuracy and completeness of the record is so important; and
- How to update information and how to add information in from other sources.

5.1.2 File naming and organisation

It is important to **name** and organise **files** in a consistent and descriptive manner so that it is obvious where to find specific data and information.

Best Practice 1: Keep file names short but meaningful

- File names should be kept as short as possible but still be meaningful
- Long file names create long file paths and long URLs
- Searches break down when a file path or URL exceeds 255 characters
- Long filenames are more difficult to remember and recognise and their associated URLs are more difficult to transmit in emails as they often ‘break’
- Avoid using initials, abbreviations and codes that are not commonly understood

Best Practice 2: Avoid repetition and redundancy

- Avoid redundancy in file names and file paths. Unnecessary repetition increases the length of file names and file paths e.g., Incorrect file name: /…/Committee/20161121CommitteMinutes.doc, Correct file name: /…/Committee/20161121Minutes.doc

Best Practice 3: Capital letters

- Use capital letters to delimit words instead of spaces and underscores e.g., ‘Naming_tutorial.doc’ should be ‘NamingTutorial.doc’.
- Avoid using spaces and underscores in file names
- Web-based applications replace spaces with the percent sign (%), which makes the path difficult to read
- Using underscores and hyphens in your file names increases the length, which is incompatible with Best Practice 1
- Where capitalised acronyms are used in file names the acronym should appear in capitals and the first letter of the following word should also be capitalized

Best Practice 4: Numbers in file names

- When including a number in a file name always use a two-digit number, unless it is a year or another number with more than two digits
- The file directory displays file names in alphanumeric order
- To maintain the numeric order when file names include numbers it is important to include the zero for numbers 0-9 to retrieve the latest record number

Best Practice 5: Dates

- Dates should always be presented ‘back to front’, that is with the year first (always given as a four digit number), followed by the month (always given as a two digit number), and the day (always given as a two digit number)
- Entering the dates back to front means that the chronological order of the records is maintained when the file names are displayed in a SharePoint list. This helps when trying to retrieve the latest dated record

Best Practice 6: Personal names

- It may be appropriate to include within a file name the name of an individual, usually when the record is a piece of correspondence
- It will not usually be appropriate to name records after the record owner or creator, i.e. avoid naming records after yourself
- When it is appropriate to include a personal name it should be given as family name first followed by initials as it is most likely that the record will be retrieved according to the family name of the individual

Best Practice 7: Do not begin file names with common words

- Avoid using common words such as ‘draft’ or ‘letter’ at the start of file names, or all of those records will appear together in a SharePoint list, making it more difficult to retrieve the records you are looking for
- You may only ignore this Best Practice if starting file names with these sorts of words aids the retrieval of the records See Best Practice 8 for further details

Best Practice 8: Word order in file names

- The elements to be included in a file name should be ordered according to the way in which the record will be retrieved during the course of everyday business
- This will depend on the way you work. For example, if the records are retrieved according to their date, the date element should appear first. If the records are retrieved according to their description, the description element should appear first

Best Practice 9: Naming recurring events files

- The file names of records relating to recurring events (e.g. meeting minutes and papers, weekly, monthly or annual reports, event management and budget planning documents) should include both the date and the event name or event description so that the record can be identified and retrieved
- When deciding the order of the elements consider Best Practice 8. Date first will usually be appropriate for events that are time specific and recurring. Event first will usually be appropriate for events that are infrequent, but regularly recurring.

- The event description could be the title of the event or the subject of the event. Whichever description type you choose, ensure that it is short, to the point, and readily recognizable to you and the colleagues you work with

Best Practice 10: Naming correspondence files

- The file names of correspondence should include the name of the correspondent, an indication of the subject, the date of the correspondence and whether it is incoming or outgoing correspondence, except where the inclusion of any of these elements would be incompatible with Best Practice 2: Avoid Repetition and Redundancy.
- The file names of correspondence should include the following elements so that the record can be easily identified and retrieved:
- Name of correspondent, that is the either the name of the person who sent you the letter/email/memo or the name of the person to whom you sent the letter/email/memo
- Subject description, where it is not given in the folder title
- Date of letter/email/memo
- If incoming correspondence, include 'rcvd' (for 'received')
- When deciding the order of the elements consider Best Practice 8. It will usually be appropriate to order the elements in the same order in which they are listed above, as it is likely that correspondence will be retrieved on the basis of the correspondent.
- If more than one email is received from the same person, on the same day, on the same subject and the latest email does not include the whole string of the correspondence, the time of the email can be included in the file name to differentiate it from the email received earlier in the day.

5.2 Use

The use of personal information needs to be defined correctly if staff do not want to be in breach of the Data Protection Act 1998. The second principle of the Act states: 'Personal data shall be obtained only for one or more specific and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.'

Without clarity regarding why that information was obtained, what it is used for and by whom, it is all too easy for it to be inadvertently reused in a way which the data subject may not be comfortable with or which damages their interests.

All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the Chief Nurse, Medical Director, Director of Health Informatics, Head of Information Governance, Health Records Manager or Information Asset Owner.

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time.

Information Asset Owners should ensure they have a business continuity plan that provides protection for records which are vital to the continued functioning of the Trust.

Where paper records need to be moved from their designated storage area they must be tracked and the tracking mechanism must record as a minimum:

- The record reference number or identifier;
- A description of the record (e.g., the file title);
- The person, position or operational area having possession of the record;
- The date of movement.

5.2.1 Network drives

Trust staff will have access to a number of shared network drives and folders, access to which is controlled by the relevant Information Asset Owner. In addition most staff are provided with a personal H:Drive. Trust records must not be held on local device Hard Drives (C:Drives), or on these private drives on the network (H:Drives). Records held in electronic format and saved on shared drives have regular back-up copies scheduled and undertaken on a daily basis.

The H:Drive should only be used for work in progress which is not yet suitable for sharing with other staff. Documents which have not become records may be stored on the private drive in the early stage of development but must be transferred to a shared drive once they are open to consultation or become records. No documents should be stored on a device hard drive.

Personal data must not under any circumstances be stored on Trust equipment, local and network drives and Trust issued storage devices.

Personal data found on Trust drives will be deleted without notice to the owner.

Upon termination of employment contents of the H:Drive will be deleted and device hard drives may be checked and any documents stored thereon will also be deleted.

Although intended for personal use the Trust reserves the right to examine the content on an H:Drive during or after termination of employment to locate and retrieve any Trust documents or records which may have been stored thereon in contravention of the above guidance. Access may be authorised by the appropriate Information Asset Owner, the Head of Information Governance, the Director of Health Informatics, the Medical Director or the Chief Nurse. Every effort will be made not to access or view any genuinely personal material.

Further guidance on the use of Trust ICT systems is available at in the Trust ICT Acceptable Use Policy and Procedure [RWF-OPPCS-NC-TM8].

5.2.2 Access and disclosure

Controlling access to information is necessary for several reasons:

- It prevents staff from being overloaded with information which they do not need to see;
- It protects crucial information from accidental modification or loss; and
- It protects personal data, commercially sensitive information and/or interests of third parties.

Specific guidance in relation to access to health records is available in the Health Records Policy and Procedure and associate standing operating procedures.

There is a range of statutory provisions that give individuals the right of access to information created or held by the Trust such as Freedom of Information requests (including correspondence on how a decision was made) and a data subject access request. The Trust will comply with its legal obligations under the Data Protection Act 1998, the Freedom of Information Act 2000, the Access to Health Records Act 1990. For further details see the Data Protection and Confidentiality Policy, Health Records Policy and associated Standard Operating Procedures and the Freedom of Information Act 2000 Policy.

There is a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties, and similarly a range of provision that require or permit disclosure. Only the specific information required should be disclosed and always in accordance and with strict adherence to the Data Protection Act 1998.

Any proposed disclosure of confidential patient information, to a third party with whom no information sharing agreement is currently in place, should be referred to the Head of Information Governance.

All decisions to disclose information should be informed by the Department of Health publication Confidentiality: NHS Code of Practice.

Staff are reminded that altering, defacing, blocking, erasing, destroying or concealing any record with the intention of preventing the disclosure or all, or any part, of the information within it, pursuant to a valid request under the Freedom of Information Act 2000 or the Data Protection Act 1998 is a criminal offence under Section 77 of the Freedom of Information Act 2000.

5.2.3 Security

Information needs to be secure at all times. All staff are reminded of things that anyone can do, to ensure security of information which include, but is not limited to the following:

- Locking confidential and sensitive information away when leaving the office unattended;
- Using complex passwords;
- Hiding laptops in cupboard or a drawer when leaving the office.

Information security is a complex topic. Further guidance can be obtained from the Security Policy and Procedure.

5.2.4 Data / information transfer

The mechanisms for transferring information from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held.

Staff members should make a record of any disclosures made including details of what was disclosed and to whom and when.

Where records are mislaid or lost reasonable searches should be made. If the records are not located after a thorough search a note should be made recording when the absence was noted and what searches were made. This should be kept in an accessible location for future reference until such time as the original records would have been disposed. All cases of lost or missing records should be logged as an incident on Datix. Further guidance is available relating to Locating Missing Case Notes and Missing Case Note Audit Trail. See Appendix 6.

5.2.5 Collaborative working

The Trust will ensure that records shared with other bodies, or held on their behalf, are managed in accordance with relevant Codes of Practice. This will be done through agreements and protocols which specify:

- What information should be contributed and kept, and by whom
- What level of information security should be applied;
- Who should have access to the records;
- What disposal arrangements should be in place;
- Which body holds the information for the purposes of the Freedom of Information Act 2000;
- Under what conditions, information will be shared or passed.

5.2.6 Closure

Records should be closed (i.e., made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes.

An indication that a file of paper records, or folder of electronic records, has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders.

Where possible, information on the intended disposal of electronic records should be included in the metadata when the information is created. The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

5.3 Retention

The Trust has adopted the Records Retention and Disposal Schedule contained in the Information Governance Alliance Records Management Code of Practice (NHS). See Appendix 7. Any decisions to vary the provisions of this schedule must only be made by the Information Asset Owner following consultation with the Head of Information Governance. The decision and the reason for it must be recorded.

Records must be reviewed to ascertain whether they need to be kept for longer than might appear from their underlying retention period or are worthy of permanent archival preservation. Certain records created by the Trust may be of historic interest.

Records selected for archival preservation and no longer in regular use by the Trust should be transferred to the Trust's approved 'Place of Deposit' (Kent County Archives based at Maidstone Library) as soon as possible and no later than the period currently required under Section 3(4) of the Public Records Act 1958 as amended by Section 45 of the Constitutional Reform and Governance Act 2010.

It is the responsibility of a staff member who is leaving their current post or the organisation, and their line manager, to identify as part of the exit procedure specific records that should be retained. These records should then be transferred securely to the requisite network drive.

5.4 Disposal

Records should not be kept longer than is necessary and should be disposed of at the right time. If the Trust continues to hold information which we do not have to keep we would be liable to disclose it if a request was received under either the Data Protection Act 1998 or Freedom of Information Act 2000. The fifth principle of the Data Protection Act 1998 also requires that personal information should not be retained longer than is necessary.

Short-lived documents such as telephone messages, notes on pads, post-its, email messages etc., which have no business significance do not need to be kept as records and should be disposed of in a secure manner having regard for the nature of the information contained therein. If they are business critical they should be transferred to a more formal location and saved as a record.

When disposing information that amounts to a record a destruction log must be compiled. This should detail:

- What information has been destroyed (by giving the information a meaningful title);
- When the information was destroyed;
- Who carried out the disposal and under whose authority.

Paper records that are neither ‘sensitive’ nor ‘confidential’ and that do not contain corporate or person identifiable information may be disposed of via ‘black bin’ waste. Paper records that do contain personal data or other confidential information must be disposed of securely. For paper records this normally involves shredding, pulping and/or incineration. Records requiring this method of disposal must be placed in one of the dedicated confidential waste bins located around the Trust.

For electronic records these should be deleted from the holding system, beyond any possibility of reconstruction. Staff should be aware that destruction is not complete until the current cycle of IT server backups is complete as the deleted records may be available from the backup archives. Such backup copies may be subject to the duties of disclosure in the Freedom of Information and Data Protection Acts.

Removable media such as memory sticks, CDs, DVDs, Floppy Disks and Hard Drives must be destroyed through secure IT disposal. Staff should contact the IT Helpdesk if any such devices are to be disposed of. The IT department will arrange for removable media to be degaussed and shredded on site.

When records are destroyed by a commercial third party such arrangements will be subject to formal contract and will require the return to the Trust of Certificates of Destruction.

APPENDIX 1

Process requirements

1.0 Implementation and awareness

- Once ratified the PRC Chairman will email this policy/procedural document to the Clinical Governance Assistant (CGA) who will activate it on the Trust approved document management database on the intranet, under ‘Policies & Q-Pulse’.
- A monthly publications table is produced by the CGA which is published on the Trust intranet under ‘Policies & Q-Pulse’; notification of the posting is included on the intranet “News Feed” and in the Chief Executive’s newsletter.
- On reading of the news feed notification all managers should ensure that their staff members are aware of the new publications.
- Information Asset Owners will be appraised of their responsibilities under this policy.

2.0 Monitoring compliance with this document

- The Trust will audit records management in a minimum of four corporate working areas per year as required by the Information Governance Toolkit Requirement 604.
- Records Management will be monitored by the Information Governance Committee.
- Audit outputs may be reviewed by TIAA as a component of the annual Information Governance Toolkit Evidence Audit.
- The Trust will use external reports to benchmark its data quality against similar organisations. These will include by not necessarily be restricted to the following:
    - NHS Digital Data Quality Reports
    - SUS Data Quality Reports
    - Dr Foster DQI Tool
- Clinical Coding will be audited on a regular basis by a qualified coding auditor. At least one of these audits each year will be by external auditors.

3.0 Review

This policy and procedure and all its appendices will be reviewed at a minimum of once every 3 years, following the procedure set out in the 'Principles of Production, Approval and Implementation of Trust Wide Policies and Procedures' [RWF-OPPPCS-NC-CG25].

If, before the document reaches its review date, changes in legislation or practice occur which require extensive or potentially contentious amendments to be made, a full review, approval and ratification must be undertaken.

If minor amendments are required to the policy and procedure between reviews these do not require consultation and further approval and ratification. Minor amendments include changes to job titles, contact details, ward names etc.; they are 'non-contentious'. For a full explanation please see the 'Principles of Production, Approval and Implementation of Trust Wide Policies and Procedures' [RWF-OPPPCS-NC-CG25]. The amended document can be emailed to the CGA for activation on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse'. Similarly, amendments to the appendices between reviews do not need to undergo consultation, approval and ratification.

4.0 Archiving

The Trust approved document management database on the intranet, under 'Policies & Q-Pulse', retains all superseded files in an archive directory in order to maintain document history.

APPENDIX 2

CONSULTATION ON: Information Lifecycle Management Policy and Procedure

Job title:	Date sent dd/mm/yy	Date reply received	Modification suggested? Y/N	Modification made? Y/N
The following staff MUST be included in ALL consultations:				
Clinical Governance Assistant	24.08.16	16.09.16	Y	Y
Chief Pharmacist	24.08.16			
Staff-Side Chair	24.08.16	07.09.16	Y	Y
Emergency Planning team	24.08.16	25.08.16	N	N/A
Head of Staff Engagement and Equality	24.08.16	25.08.2016	N	N/A

Consultation process – Use this form to ensure your consultation has been adequate for the purpose.

Please return comments to: Head of Information Governance (GSpinks@nhs.net)

By date: 15 September 2016

Health Records Manager	24.08.16			
All individuals listed on the front page of this document	24.08.16			
All members of the approving committee: Information Governance Committee	24.08.16	24.11.16	Y	Y
All Information Asset Owners	24.08.16			
The following staff have consented to have their name included within this policy and any associated appendices: Gail Spinks, Head of Information Governance				

APPENDIX 3

Equality impact assessment

In line with race, disability and gender equalities legislation, public bodies like Maidstone and Tunbridge Wells NHS Trust are required to assess and consult on how their policies and practices affect different groups, and to monitor any possible negative impact on equality. The completion of the following table is therefore mandatory and should be undertaken as part of the policy development and approval process. **Please note that completion is mandatory for all policy and procedure development exercises.**

Title of policy or practice	Information Lifecycle Management Policy and Procedure
What are the aims of the policy or practice?	To set out the framework for effective information and record management within the Trust
Identify the data and research used to assist the analysis and assessment	Best practice guidance available from the Information Governance Toolkit; The NHS Code of Practice for Records Management.
Analyse and assess the likely impact on equality or potential discrimination with each of the following groups.	**Is there an adverse impact or potential discrimination (No).** **If yes give details.**
Males or females	No
People of different ages	No
People of different ethnic groups	No
People of different religious beliefs	No
People who do not speak English as a first language	No
People who have a physical disability	No
People who have a mental disability	No
Women who are pregnant or on maternity leave	No
Single parent families	No
People with different sexual orientations	No
People with different work patterns	No

(part time, full time, job share, short term contractors, employed, unemployed)	
People in deprived areas and people from different socio-economic groups	No
Asylum seekers and refugees	No
Prisoners and people confined to closed institutions, community offenders	
Carers	No
If you identified potential discrimination is it minimal and justifiable and therefore does not require a stage 2 assessment?	No potential discrimination was identified.
When will you monitor and review your EqIA?	Alongside this policy/procedure when it is reviewed.
Where do you plan to publish the results of your Equality Impact Assessment?	As Appendix 3 of this policy/procedure on the Trust approved document management database on the intranet, under 'Trust policies, procedures and leaflets'.

FURTHER APPENDICES

The following appendices are published as related links to the main policy /procedure on the Trust approved document management database on the intranet, under 'Policies & Q-Pulse':

No.	Title	Unique ID
4	Example of audit planning document; Checklists to measure/test compliance for key components of records management; Audit outcome report	RWF-IMT-CIN-APP-1
5	Government Security Classifications (Protective Marking Scheme)	RWF-IMT-CIN-GUI-1
6	Locating missing case notes and missing case note audit trail	RWF-OPPM-CORP28
7	Information Governance Alliance Records Management Code of Practice for Health And Social Care (NHS)	RWF-IMT-CIN-GUI-2