

Records Management Policy and Procedure

Policy Number	IG005
Target Audience	CCG/GMSS Staff
Approving Committee	CCG Chief Officer
Date Approved	February 2018
Last Review Date	February 2018
Next Review Date	February 2020
Policy Author	GMSS IG Team
Version Number	V5.0

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1.1	January 2015	A Hughes	Change of Overall Responsibility
2.0	January 2017	IG Team	Changes from CSU to GMSS. Addition of section 5. NHS Numbers. Reference to Records Management Code of Practice for Health and Social Care 2016.
2.0	February 2017	IM&T Board Ops	Approved.
3.0	January 2018	IG Team	Review to incorporate the GDPR legislation
4.0	January 2018	IM&T Board Ops	Approved.
5.0	February 2018	CCG Chief Officer	Approved.

Analysis completed	of Effect	By: M Robinson	Date: August 2013
--------------------	-----------	----------------	-------------------

Contents

1.	Introduction	5
2.	Aims of a Records Management System	6
3.	Scope	7
4.	Definitions	7
5.	NHS Number	9
6.	Accountability, responsibilities and training	10
7.	Inventory of Records held	11
8.	Record Creation	12
9.	Record Quality	13
10.	Record Keeping	14
11.	Record Maintenance	15
12.	Tracking of Records	15
13.	Record Transportation	17
14.	Lost/Missing Records	18
15.	Scanning	18
16.	Disclosure and Transfer of Records	19
17.	Retention, Archiving and Disposal of Records	19
18.	Record Closure	19
19.	Retention Schedules and Record Disposal	20
20.	Classification of NHS Information within the CCG	21
21.	Freedom of Information	21
22.	Training Requirements	22
23.	Subject Access Request	22
24.	Information Risk Management	23
25.	Records Management and System Audit	23
26.	IG Training and Awareness	23
27.	Monitoring and Review	24
28.	Legislation	25
29.	Other relevant Procedural Documents	25
	Appendix 1 Checklist: Creating a Record	26
	Appendix 2 – Quality of Record Entries	27

Appendix 3 – Transportation of information log sheet	28
Appendix 4 – Procedure for handling Missing/Lost Records	30
Appendix 5 – Sending Information via Postal Service	31
Appendix 6 – Full Guidance on Retention Schedules	32
Appendix 7 – Retention Schedule	33
Appendix 8 – Classification Categories	37
Appendix 9 – Freedom of Information Act Exemptions	42

1. Introduction

- 1.1 The purpose of this document is to provide guidance to all Bolton Clinical Commissioning Group (henceforth referred to as “the CCG”) staff on Records Management. This policy is adopted from the NHS England Policy of the same name.
- 1.2 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal. The CCG has a statutory obligation to maintain accurate records of its activities and are public records under the terms of the Public Records Acts 1958 & 1967.
- 1.3 The Records Management: NHS Code of Practice has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.
- 1.4 Additionally, the implementation of the General Data Protection Regulation Protection (GDPR) requires better records management. Organisations need to know what personal data they hold, to be able to tell individuals how long they will keep it for, to be able to access it when they need to, and to keep it securely. This Records Management Policy and Procedure document aids compliance with GDPR.
- 1.5 The CCG records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the CCG and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.
- 1.6 For the purpose of this document CCG records refer to Corporate records (i.e. personnel files, minutes etc.) and clinical/health records (patient health records) where appropriate.
- 1.7 The CCG has adopted this Records Management Policy and Procedure document and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:
 - better use of physical and server space;
 - better use of staff time;
 - improved control of valuable information resources;
 - compliance with legislation and standards;
 - reduced costs

February 2018:	Page 5 of 42	Records Management Policy:	Version No: 5.0
----------------	--------------	----------------------------	-----------------

- 1.8 The CCG also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.
- 1.9 This document sets out a framework within which the staff responsible for managing the CCG's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.
- 1.10 It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy and procedure.

2. Aims of a Records Management System

- 2.1 The aims of the Records Management System are to ensure that they are:
- available when needed so that events or activities can be followed through and reconstructed as necessary;
 - accessible, located and displayed in a way consistent with their initial use, with the current version being identified where multiple versions exist;
 - able to be interpreted and set in context: who created or added to the record and when, during which business process, and how the record is related to other records;
 - trustworthy and hold integrity, reliably recording the information that was used in, or created by, the business process;
 - maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy;
 - secure from unauthorised or inadvertent alteration or erasure, with access and disclosure being properly controlled and audit trails tracking use and changes;
 - held in a robust format which remains readable for as long as records are required;
 - retained and disposed of appropriately using documented retention and disposal procedures, which include provision for appraising and permanently preserving records with particular archival value; and
 - CCG staff are trained and made aware of their responsibilities for record-keeping and record management.

February 2018:	Page 6 of 42	Records Management Policy:	Version No: 5.0
----------------	--------------	----------------------------	-----------------

3. Scope

- 3.1 This policy and procedure applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy and procedure applies to all third parties and others authorised to undertake work on behalf of the CCG.
- 3.2 This guidance relates to all clinical and non-clinical records held in any format by the CCG. A 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:
- administrative records (including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling);
 - audio and videotapes, cassettes and CD-ROMs;
 - computer databases, output, and disks, and all other electronic records;
 - photographs, slides and other images
 - scanned documents
 - any portable media containing information
 - material intended for short term or transitory use, including notes and "spare copies" of documents;
 - meeting papers, agendas, formal and informal meetings including notes taken by individuals in note books and bullet points are all subject to the above; and
 - emails and other electronic communications.
- 3.3 This list is not exhaustive.
- 3.4 **Limitations and Applications for CCG Staff** - The introduction of the Health and Social Care Act 2012 removed some of the powers and rights of commissioning organisations to obtain, handle, use and share confidential and identifiable information from the CCG. In general, CCG staff are not entitled to use Personal Confidential Data (PCD). Whilst this policy and procedure references health records, this advice is only applicable to CCG staff who have a legal right to this information, and is not applicable to all staff.
- 3.5 A document becomes a record when it has been finalised and becomes part of the organisation's corporate information.

4. Definitions

- 4.1 **Records management** is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally

February 2018:	Page 7 of 42	Records Management Policy:	Version No: 5.0
----------------	--------------	----------------------------	-----------------

sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure
- closure and transfer
- appraisal;
- archiving and disposal.

4.2 The term **records life cycle** describes the life of a record from its creation/receipt through the period of its active use, then into a period of inactive retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

4.3 In this policy and procedure, **records** are defined as “recorded information, in any form, created or received and maintained by the CCG in the transaction of its business or conduct of affairs and kept as evidence of such activity.”

4.4 **Information** is a corporate asset. The CCG records are important sources of administrative, evidential and historical information. They are vital to the CCG to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

4.5 **Corporate/business records** are defined as anything that contains information in any media, which has been created or gathered as evidence of undertaking of work activities in the conduct of business. Corporate records may also be generated through supporting patient care and can also be generated through agency/casual staff, consultants and external contractors.

4.5.1 Corporate records types include;

- Administrative records (including personnel, estates, financial and accounting, contract records , litigation and records associated with complaints- handling);
- Registers and rotas;
- Office /appointment diaries;
- Photographs, slides, plans or other graphic work (not clinical in nature);
- Micro film a (i.e. fiche/film);
- Audio and video tapes; and
- Records in all electronic formats including emails.

February 2018:	Page 8 of 42	Records Management Policy:	Version No: 5.0
----------------	--------------	----------------------------	-----------------

- 4.6 A health record is defined as being any record which consists 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 the individual.

5. NHS Number

- 5.1 The NHS Number is a unique number given to every baby born in England and patient registered with the NHS and is the prime patient identifier. This patient identifier enables clinical and administrative records to be exchanged more safely between both electronic and manual systems.
- 5.2 The CCG will ensure that NHS numbers are used on all clinical communications, clinical records and on all systems processing patient information.
- 5.3 And will further ensure the following principals are applied when processing patient information and will not procure any IT system that does not support these principals.

5.4 NHS Number Principles

5.4.1 Find It

- Find / Request the NHS Number on referral letters / forms received;
- Determine and verify the NHS Number before or at the start of an episode of care;
- If this is not possible then tracing should be performed as early as possible in the episode either at point of contact or as a back office process.

Use It

- Use the NHS Number to search for an electronic record as the 'First Choice';
- Use the NHS Number to identify people presenting for care;
- Include the NHS Number on electronic records, wristbands, notes, forms, letters, document and reports which include patient information and are used for that person's care;
- Use the NHS Number as the key identifier for service users;
- Ensure systems can support the NHS Number;
- Use the Personal Demographics Service (PDS) or Demographics Batch Service (DBS) to trace NHS Numbers;

Share It

- Include in all communications, written, verbal and electronic, during telephone calls, on all letters, referrals, forms, documents;
- Internally within your organisation and with all other organisations you contact as part of the provision of care;
- Ensure the NHS Number is included when providing users with any letters or forms;
- Supply the NHS Number as the key identifier for any patient information that assess across systems and organisation boundaries.

February 2018:	Page 9 of 42	Records Management Policy:	Version No: 5.0
----------------	--------------	----------------------------	-----------------

6. Accountability, responsibilities and training

- 6.1 Overall responsibility for the Records Management Policy and Procedure lies with the Chief Officer who has overall responsibility for managing the development and implementation of records management procedural documents and for working with the Greater Manchester Shared Services (GMSS) Information Governance (IG) Team who will provide some Records Management advice and guidance in line with their contractual obligations.
- 6.2 The Caldicott Guardian is the conscience of the organisation and is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential personal information are in place. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.
- 6.3 The SIRO (Senior Information Risk Owner), under delegated authority from the Chief Officer will oversee compliance with the GDPR and Data Protection Act (DPA) and the development of appropriate policy and procedure. The SIRO will be advised by supported by GMSS IG Team. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.
- 6.4 Information Asset Owners (IAOs)/Administrators (IAAs) under the responsibility of the SIRO will:
- be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
 - ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
 - be responsible for the Information Asset assigned to them;
 - ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a Subject Access Request;
 - ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy and Procedure, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.
- 6.5 Data Protection Officer (DPO)

The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct

February 2018:	Page 10 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

internal audits. In addition they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

- 6.6 The Governance, Risk & Complaints Manager is responsible for co-ordinating, publicising, implementing and monitoring the Records Management Policy and Procedure and reporting issues or concerns to the CCG's IM&T Operations Board when required.
- 6.7 Directors and senior managers are personally accountable for the quality of records management within the CCG and all line managers must ensure that their staff, whether administrative or clinical, are adequately trained and apply the appropriate guidelines, that is, they must have an up-to-date knowledge of the laws and guidelines concerning confidentiality and data protection.
- 6.8 The CCG's IM&T Operations Board will be responsible for ensuring that this policy and procedure is implemented, through the Records Management Policy and Procedure, and that the records management system and processes are developed, co-ordinated and monitored.
- 6.9 All CCG employees (including temporary and contract staff), whether clinical or administrative, who create, receive and use records in any form of media have records management responsibilities. In particular all staff must ensure they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and with any guidance. Furthermore, any record that any individual creates is a public record and may be subject to both legal and professional obligations, including compliance with relevant legislation included the Freedom of Information Act, the Data Protection Act and GDPR. This responsibility is established at, and defined by, the law (Public Records Act 1958).
- 6.10 Staff will receive instruction and direction regarding the policy from a number of sources:
- policy/strategy and procedure manuals;
 - line manager;
 - other communication methods (e.g. team brief/team meetings); and
 - staff Intranet.

All staff are mandated to undertake the "Introduction to Information Governance" e-learning module. Information Governance training is required to be undertaken on an annual basis.

7. Inventory of Records held

February 2018:	Page 11 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

- 7.1 The CCG will establish and maintain mechanisms through which Directorates and other units can document the records they are maintaining. The inventory of record collections will facilitate:
- the classification of records into series; and
 - the recording of the responsibility of individuals creating records.
- 7.2 The register will be reviewed annually with the support of the IG team.

8. Record Creation

- 8.1 The CCG should have a process for documenting its activities, taking into account the legislative and regulatory environment in which it operates.
- 8.2 Records must hold adequate 'integrity' so their evidential weight is legally admissible, and can withstand scrutiny in the event of litigation or claim. True and accurate records protect the right of the individual or the CCG.
- 8.3 All records should be complete and accurate:
- to allow staff to undertake appropriate actions in the context of their responsibilities;
 - to protect legal and other rights of the organisation, patients, staff and other people affected;
 - to show proof of validity and authenticity.
- 8.4 Records should be created and maintained in a manner that ensures that they are clearly identifiable, accessible, and retrievable in order to be available when required. All records should have a unique number or filing system, which will be applicable only to that record. For example, a patient's medical record will be identifiable by the NHS number and an employee's personal file held in personnel number. Records must have clear and precise formats and must be structured in the same way that files of the same description are structured with an easy to follow standard index, either numerical, by date or alphabetically.
- 8.5 The following should be documented when a paper or electronic record is created:
- file reference;
 - file title;
 - if appropriate protective marking i.e. Customer Confidential/CCG Confidential;
 - if possible an anticipated disposal date and what action to take;
 - where action cannot be anticipated, mechanisms must be in place to ensure this action takes place when the file is closed;
 - all filing systems to be documented and kept up to date.
- 8.6 Managers of departments should ensure staff are made aware of their responsibilities, are properly trained and that reviews and monitoring for compliance are undertaken.

February 2018:	Page 12 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

- 8.7 All major decisions or key actions which may result from discussions or meetings should be recorded as this provides key evidence of business of business decision making activity.
- 8.8 The CCG will ensure consistency is established in the way information is presented to target audiences, both internally and externally. When creating a record the CCG will need to achieve the following:
- 8.9 Hold the necessary records to enable staff to perform their duties;
- ensure information can be located promptly and time wasted on locating or recreating lost documents reduced;
 - appropriate disclosure of information to staff or the public who require and are authorised to access;
 - evidence of individual and corporate performance and activity;
 - physical and digital space is used effectively;
 - records created are able to meet the CCG's legal obligations;
 - organisations can preserve its corporate memory and track business decisions or transactions over time.
- 8.10 For checklist on how to create a Record refer to Appendix 1, Checklist; Creating a Record.

9. Record Quality

- 9.1 All CCG staff should be fully trained in record creation use and maintenance, consummate to their roles, including having an understanding of what should be recorded and how it should be recorded and the reasons for recording it. Staff should know:
- how to validate the information with the patient or the carer or other records to ensure they are recording the correct data;
 - why they are recording it;
 - how to identify, report and correct errors;
 - the use of the information and record;
 - what records are used for and the importance of timeliness, accuracy and completeness;
 - how to update and add information from other sources.
- 9.2 Full and accurate records must possess the following three essential characteristics:
- Content – the information it contains (text, data, symbols, numeric, images or sound);
 - Structure – appearance and arrangement of the content (style, font, page and paragraph breaks, links and other editorial devices).
 - Context – background information that enhances understanding of the business environment/s to which the records relate (e.g.

February 2018:	Page 13 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

metadata, software) and the origin (e.g. address title, function or activity, organisation, program or department).

- 9.3 The structure and context of each record will alter depending on the record being created. For example, policies will need to hold contextual information like author names, review date and ratification information; whereas agenda does not require that type of information but should include attendees, venue, date and time.

9.4 Quality Checking

The CCG should establish quality checks which will minimise/eradicate errors. A different member of staff should quality check to the one that has input the information. Dependent on the type of record the following checks should be undertaken:

- ensure the correct retention period has been input onto the document which confirms the right retention/destruction will have been calculated;
- ensure all names are spelt correctly and in the correct format;
- ensure the unique identifiers are correct and in the right format;
- check the barcode number is correct (if relevant);
- the inventory should be checked for all other possible errors.

For further information on how to check the quality of a record refer to Appendix 2 – Quality of Record entries.

10. Record Keeping

- 10.1 Implementing and maintaining an effective records management service depends on knowledge of what records are held, where they are stored, who manages them, in what format(s) they are made accessible, and their relationship to organisational functions. An information inventory or record audit is essential to meeting this requirement. The inventory will help to enhance control over the records, and provide valuable data for developing records appraisal and disposal policies and procedures.
- 10.2 Paper and electronic keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.
- 10.3 All records must conform to these record keeping guidelines, legislation, NHSLA, DoH, Information Governance requirements and professional guidelines.

February 2018:	Page 14 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

11. Record Maintenance

- 11.1 The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.
- 11.2 Storage accommodation for current records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.
- 11.3 For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.
- 11.4 Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.
- 11.5 When paper records are no longer required for the conduct of current business, their placement in a designated secondary storage area may be a more economical and efficient way to store them. Procedures for handling records should take full account of the need to preserve important information and keep it confidential and secure. Archiving policies and procedures should be observed for both paper and electronic records.
- 11.6 All individual files should be weeded on a regular basis, to ensure the key documentation is readily identifiable and accessible. Bulky files should contain no more than 4 years' worth of records. Any file older than this should be culled and removed to an inactive file. The front cover of each such volume must clearly indicate that other volumes exist.
- 11.7 Any duplicate documents (except where copy letters sent or received have had comments added by hand) should be culled and confidentially destroyed.
- 11.8 In order to identify when records were last active or the service user was last in contact with the service, it is advisable that year labels are used on the front cover.
- 11.9 If there are separate sets of records relating to the same service user which is a consequence of historic practice, these should all be stored together upon discharge and kept together when archived.
- 11.10 A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation.

12. Tracking of Records

- 12.1 Accurate recording and knowledge of the whereabouts of all clinical and non-

February 2018:	Page 15 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

clinical records is essential if the information they contain is to be located quickly and efficiently. Records must not be taken out of the office unless this has been agreed by the Line Manager and a tracking mechanism is in place. The tracking system could be manual or electronic and linked to a department's IT system.

12.2 Tracking mechanisms should record the following (minimum) information:

- The item reference number of the record or other identifier;
- a description of the item (e.g. file title);
- the person, unit or department, or place to whom it is being sent;
- the date of the transfer to them;
- the date of the information returned (if applicable).

12.3 Manually operated tracking systems are common methods for manually tracking the movements of active records and include the use of:

- a paper register – a book, diary, or index card to record transfers, item reference number of the record or other identifier;
- file “on loan” (library type) cards for each absent file, held in alphabetical or numeric order;
- file “absence” or “tracer” cards put in place of absent files.

12.4 Electronically operated tracking systems include:

- a computer database, excel spread sheet in place of paper/card index;
- bar code labels and readers linked to computers;
- work flow software to electronically track documents.

12.5 The minimum data which needs to be recorded includes:

- service user's name;
- NHS number;
- date the records were removed,;
- destination and name of intended recipient;
- name of the person releasing the records.

12.6 A well thought out, manual or electronic system should:

- provide an up-to-date easily accessible movement history and audit trail;
- be routinely checked and updated;
- be recorded i.e. all movements of a record even if the record is exchanged between teams/staff members within the same building;
- provide a return receipt and it made clear to whom the records should be returned ;
- ensure information recorded on the tracking system must be correct and applicable to ensure the system remains effective;
- take into consideration any filing that comes in whilst the records are traced out and must be filed according to local documented procedures until such time as the records are returned;
- ensure that any records are returned safely to their correct home and absent records are chased on a frequent basis;

February 2018:	Page 16 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

- maintain a log of all records received into the department including the date received, service user name and NHS number.

12.7 Managers should ensure that training and procedures are in place for manual and electronic tracking systems and that they are being adhered to.

13. Record Transportation

13.1 All CCG employees and contractors have a legal duty to keep information safe and secure. Security and confidentiality of records should be paramount at all times. This is particularly important, in high security risk situations such as the transportation of records between sites. Records should not be taken off site without the authorisation of the relevant line manager. To reduce the risk of loss of records and the risk of breaches of confidentiality staff are advised to observe the following minimum precautions:

- Records should be tracked out of the respective department so that other staff are aware of the location of the record;
- records should never be left unattended where it would be possible for an unauthorised person to have access to them;
- records being transported should always be kept out of sight;
- if records are taken home, they must be stored securely in accordance with the staff members Professional Code of Conduct.

13.2 NHS organisations are required to map their information flows in accordance with the guidance in the Information Mapping Tool. The objective of this is to demonstrate that an organisation, in this case the CCG, clearly identifies and has addressed the risks associated with the transfer of identifiable information. This mapping requires all organisations to have an up to date register of information transfers (i.e. audit or map the flows of information in and out across the organisation).

13.3 Offsite movement of records or other confidential/sensitive information.

13.3.1 Security requirements also apply when staff records are transported. It is recognised that staff may find it necessary to remove records from their base, to ensure business continuity. To reduce the risk of loss of such records and to reduce the risk of breaches of confidentiality there are various considerations to be made, based on best practice:

- Records should not be removed for administrative purposes i.e. writing reports. A trace should be kept at the base from which records have been removed and staff are aware of the location of the record;
- Records should not be left unattended in cars;
- Records kept in any staff possession should remain safe and secure at all times i.e. out of sight and locked away when not in use;
- Records should only be taken off site with the approval of the Line Manager;

February 2018:	Page 17 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

- Any vehicle used for the transportation of records must be insured for business use. If the staff member is involved in a road traffic accident which necessitates the car being left on the roadside or taken to a garage, records should be removed.
- If this is not possible the matter should be reported to the Line Manager and an incident form completed.

13.4 Appendix 3 – Transportation of information log sheet. This should be used when transporting any records from one place/organisation/department to another.

13.5 For information and procedures on posting records/sensitive information refer to Appendix 5.

14. Lost/Missing Records

14.1 A lost/missing record is a record either that cannot be found following a search in the office environment or is unavailable.

14.2 The loss of records constitutes a reportable incident and should be reported in accordance with the CCG's Incident Reporting Procedure.

14.3 It is important that records can be retrieved at any time during the retention period, whether for management or legal purposes.

15. Scanning

15.1 For reasons of business efficiency and in order to alleviate storage space/issues, the CCG can scan into electronic format inactive records which exist in paper format. The following factors should be taken into account:

- the costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
- 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
- the need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).

15.2 In order to fully realise the benefits of reduced storage requirements and business efficiency, the CCG will securely dispose of the paper records that have been copied into electronic format and stored in accordance with appropriate standards.

February 2018:	Page 18 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

16. Disclosure and Transfer of Records

- 16.1 There are 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 provisions that require or permit disclosure. Guidance should be sought from the GMSS IG Team prior to any disclosure. If the request for access to information is made under the Freedom of Information Act 2000, then the request should immediately be forwarded to the Governance, Risk and Complaints Manager within the CCG in order to comply with the deadlines specified in the Act.
- 16.2 The Caldicott Guardian should be made aware of any proposed disclosure of confidential patient information, informed by the Department of Health publication Confidentiality: NHS Code of Practice.
- 16.3 The mechanisms for transferring records from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held. The GMSS IG Team can advise on appropriate safeguards.

17. Retention, Archiving and Disposal of Records

- 17.1 Appraisal refers to the process of determining whether records are worthy of additional retention or permanent archival preservation. If the latter, this should be undertaken in consultation with the National Archives, or with an approved Place of Deposit where there is an existing relationship.
- 17.2 The purpose of the appraisal process is to ensure that the records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for a longer period as they are still in use, or whether they should be destroyed.
- 17.3 The procedure for recording the disposal decisions made following appraisal must be followed. The CCG will determine the most appropriate person(s) to carry out the appraisal in accordance with the retention schedule. This should be a senior manager with appropriate training and experience who has an understanding of the operational area to which the record relates.
- 17.4 Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility.

18. Record Closure

- 18.1 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

February 2018:	Page 19 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

reference purposes. Each year a list of records coming to the end of their retention period should be reviewed. 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 record is created.

- 18.2 Records/information contain personal confidential information and it is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and complete illegibility is secured. Destruction of all records, regardless of the media in which they are held should be conducted in a secure manner ensuring safeguards are in place against accidental loss or disclosure.

19. Retention Schedules and Record Disposal

- 19.1 It is a fundamental requirement that all of the CCG's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to CCG's business functions.
- 19.2 The CCG has adopted the retention periods set out in the Records Management: NHS Code of Practice for Health and Social Care 2016. These retention schedules outline the recommended minimum retention period for NHS records.
- 19.3 Senior Managers will be responsible for ensuring disposal schedules are implemented as part of a rolling programme. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry to the document. i.e. a file's first entry is in February 2001 and the last December 2006, the minimum retention period is eight years, it should therefore be kept in its entirety at least until 31st December 2014. If a member of staff feels that a particular record needs to be kept for longer than the recommended minimum period or there is a specific purpose further advice and approval should be sought from the Service Senior Manager/Director.
- 19.4 Where there are records held by the organisation that do not have a retention period advice should be sought from the IM&T Operations Board where approval and inclusion of the retention period will be granted.
- 19.5 Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution that has adequate storage and access facilities. Non-active records should be transferred no later than 30 years from creation of the record, as required by the Public Records Act.
- 19.6 Records not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as

February 2018:	Page 20 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

is appropriate to the level of confidentiality or protective markings they bear.

- 19.7 The methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. Contractors, if used, are required to sign confidentiality undertakings and to produce written certification as proof of destruction.
- 19.8 A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the CCG, thus making the CCG aware of any destroyed records.
- 19.9 If a record due for destruction is the subject of a statutory request for information or potential legal action, destruction should be delayed until disclosure has taken place or the legal process complete. Advice should be obtained from the Information Governance Lead.
- 19.10 It must be remembered that the destruction of records is an irreversible act.
- 19.11 Please see Appendix 7 - Retention Schedule for further details.

20. Classification of NHS Information within the CCG

- 20.1 The aim of the Classification Marking of NHS Information is to demonstrate 'good practice' in marking the records for which the CCG are responsible.
- 20.2 This is applicable for information recorded on paper and that processed electronically including printouts, reports etc.
- 20.3 Through the application of this policy and procedure, the CCG will be able to further demonstrate the effectiveness of their local IG practices.
- 20.4 This policy and procedure should be considered alongside the following:
- NHS Codes of Practice and guidance on Confidentiality
 - Information Security Management
 - CCGs Acceptable Use Policy (Inc IT, Email and Internet)
- 20.5 This policy sets out a proposed simple scheme of classification relevant to the needs of the CCG.
- 20.6 Please see Appendix 8 for details of the Classification Categories.
- 20.7 All staff working in the CCG are responsible for managing the documents and records they create or use in performance of their duties.

21. Freedom of Information

- 21.1 When classifying NHS documents regard should be paid to the requirements

February 2018:	Page 21 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

of the Freedom of Information Act 2000.

- 21.2 Consideration should be given before marking documents that would normally be published or disclosed on request. Over-classification might lead to inappropriate decisions not to disclose information that would later be embarrassing to the CCG.
- 21.3 Protective markings should wherever possible be restricted to information that would be exempt from disclosure, including temporary exemptions, such as the drafts of documents that are intended for publication.
- 21.4 A note of the exemptions that might be relevant to the protective markings is included in Appendix 9.
- 21.5 On receipt of Freedom of Information requests CCG staff should forward onto their CCG FOI Lead for guidance. It is rare that staff will receive requests directly, requestors are advised to contact the Patients Services within GMSS.

22. Training Requirements

- 22.1 A training needs analysis will be undertaken with staff affected by this document. Classification Marking of NHS Information
- 22.2 Based on the findings of that analysis appropriate training will be provided to staff as necessary.

23. Subject Access Request

- 23.1 A Subject Access Request, commonly referred to as a SAR is a request from a data subject to see a copy of, personal information that is held about them as an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the CCG, both in electronic and paper files, this is known as a SAR.
- 23.2 Any individual is entitled to:
- Know what information is held about them and why;
 - Gain access to it regardless of the media which it is held;
 - Have their information kept up to date;
 - Require the CCG to rectify/block, erase or destroy inaccurate information;
 - Not have processed confidential information about them likely to cause damage or distress;
 - Not have processed confidential information about them for the purposes of direct marketing
- 23.3 In most cases the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent

February 2018:	Page 22 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

may be needed. It may be a condition of patients, and employment of staff, that they agree to the CCG processing of specific classes of personal information.

23.4 The CCG may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety, or comply with the requirements of other legislation.

23.5 For further guidance and information please see the CCG's Subject Access Request Procedure.

24. Information Risk Management

24.1 Where required the information risk management process will take place using the NHS "5x5 Risk Matrix" as detailed in the NPSA's "Risk Matrix for Risk Managers". The Information Risk Policy contains guidance on how to interpret the scores that will be attributed to risks and provide the basis for information risk reporting to the CCG's IM&T Operations Board and Executive Team.

25. Records Management and System Audit

25.1 The process for monitoring and evaluating the effectiveness of this policy, including obtaining evidence of compliance will be part of the Information Governance annual self-assessment audit process (IG Toolkit). The CCG will regularly audit its records management practices for compliance with the framework.

25.2 The audit will:

- identify areas of operation that are covered by the CCG policies and identify which procedures and/or guidance should comply to the policy;
- follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made;
- set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance: and
- highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment related procedures.

25.3 The results of audits will be reported to the relevant quality and standards groups within the CCG under designated authority from the CCG's IM&T Operations Board and Executive Team.

26. IG Training and Awareness

26.1 Information Governance training must be undertaken on an annual basis. CCG staff are mandated to undertake the mandatory Information Governance

February 2018:	Page 23 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

annually. Records Management features in this training. All CCG Staff will be made aware of their responsibilities for record-keeping and record management.

- 26.2 Where staff may take on a specific Information Governance roles within the CCG e.g. Records Manager, additional Information Governance training will be required. For further guidance refer to the CCG's Training Needs and Analysis (TNA) Document.
- 26.3 The Information Governance Training will be utilised and uptake will be monitored. Where necessary the CCG can request ad-hoc face to face training sessions relating to Records Management this will be co-ordinated by the GMSS IG Team.
- 26.4 The CCGs IM&T Operations Board will be responsible for ensuring that this policy and procedure is implemented, and that the records management system and processes are developed, co-ordinated and monitored.
- 26.5 This policy and procedure will be placed on the CCG's website for all staff to access.
- 26.6 To maintain high staff awareness the CCG will direct staff to a number of sources:
- policy/strategy and procedure manuals;
 - line manager
 - specific training courses
 - other communication methods, for example, team meetings; and staff Intranet.

27. Monitoring and Review

- 27.1 This policy and procedure will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit
- 27.2 This policy and procedure will be reviewed on a two yearly I basis, and in accordance with the following as and when required:
- legislative changes;
 - good practice guidance;
 - case law;
 - significant incidents reported;
 - new vulnerabilities; and
 - changes to organisational infrastructure;
- 27.3 Where there are no significant alterations required, this Policy and Procedure shall remain for a period of no longer than two years of the ratification date.

February 2018:	Page 24 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

28. Legislation

28.1 All NHS records are public records under the Public Records Acts 1958. The CCG will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice for Health & Social Care 2016, additionally:

- The Public Records Act 1958;
- General Data Protection Regulation
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice;and
- National Archive - <http://www.nationalarchives.gov.uk/>.

28.2 The CCG will also take action to comply with any new legislation affecting records management as it arises.

28.3 Under the Freedom of Information Act 2000, once a record has been requested, it cannot be destroyed. It is a criminal offence to amend, erase or destroy information once a request is received.

29. Other relevant Procedural Documents

- Information Governance Framework
- Information Governance Policy
- Data Protection & Confidentiality Policy
- Confidentiality Audit Policy
- Information Governance & Cyber Incident Reporting Policy
- Secure Transfer of Information Policy
- Acceptable Use Policy
- Information Risk Policy
- Information Security Policy
- Subject Access Procedure

This list is not exhaustive

February 2018:	Page 25 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 1 Checklist: Creating a Record

- Check you know how to create adequate records and what information they should contain;
- Follow relevant CCG policies and guidelines to ensure creating full and accurate records;
- Establish and document local procedures on creating business critical records to the department, or if using a corporate or local proforma; and ensure procedures are followed;
- Use corporate templates wherever available so it clearly identifies the nature of the information and type of document;
- Include fundamental elements like author, date, title, department, contact details, and it holds the approved corporate identity;
- Ensure documents hold the relevant information specifically required for that type of record, like in the case of policies or forms. In the example of a policy this would include: executive signature, approval route, review date;
- Capture decision-making in minutes or when creating records or emails, and that you maintain a record of any transactions. For example, agreements or discussions that impact on your work or with other teams/organisations;
- Always ensure that the information you are recording is accurate and objective;
- Use standard terms to describe documents and be consistent with use of acronyms;
- Identify the creator and use their job title, plus other people who may have contributed to the document;
- Explain within the text of the document, any codes or abbreviations used, as their meaning may become less clear over time;
- Do not use logos, icons or catchphrases on documents that have been formally approved; include the CCG logo in all appropriate records;
- Remember that your records, or local record keeping practises may be required for performance checks or in the event of a claim or litigation.

February 2018:	Page 26 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 2 – Quality of Record Entries

Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice.

Good record keeping is a mark of skilled and safe practice, whilst careless or incomplete record keeping often highlights wider problems with individual practice.

Examples of good record keeping below:

- Structure and Content of Records
- Where possible there must be one set of records for each data subject/individual.
- Unique Identifier
- A unique identifier must be used to ensure that records can be retrieved when archived or stored.

Record entries should be:

- Complete
- Legible
- Contemporaneous, i.e. written as soon as possible
- Consecutive
- If appropriate, signed by the data subject/individual according to the service specific policies
- Only in exceptional circumstances, should entries to records be delayed

Abbreviations

- Abbreviations must not be used routinely.

Alterations

Contemporaneous alterations to records are acceptable when an entry has been made in error. When this occurs, the author must take the following actions:

- Make an entry stating “written in error” near the incorrect entry
- Sign, date and record the time of the annotation making the change
- Strike through the original entry with a single line leaving it discernible
- Make the correct entry, signing it and dating it

It is unacceptable to:

- Delete or erase notes, such that the entry is no longer legible
- Use correction fluids of any part of a clinical record
- Change original entries, other than as specified above
- Change entries made by another person

February 2018:	Page 27 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 3 – Transportation of information log sheet

Address for Reply

Direct Telephone Number:

Direct Fax Number:

E-Mail Address:

Description of information to be transported / list of records, folders or disc titles:

.....
.....
.....
.....
.....

Number of records / folders / discs / items:

.....

To be transported by:

Name (Print):

.....

Organisation and Designation:

.....

Contact Number:

.....

To be received by:

Name (Print):

.....

Designation:

.....

Organisation name and Address:

.....

(including postcode)

.....

Method of transportation:

.....

Estimated duration of transit:

.....

February 2018:	Page 28 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Goods received by Courier/Organisation/Department:

Date: Time:

Print Name:

Signature:

Name of CCG employee handing over the information:

.....

Designation:

.....

Contact Number:

.....

Signature: Time and Date:

.....

Goods received by: Date: Time:.....

Print Name:Signature:.....

The receiver (courier/organisation/department etc.) will immediately contact the CCG using the above contact details to confirm that the information has been successfully delivered. A copy of this form may be provided to the receiver on request.

February 2018:	Page 29 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 4 – Procedure for handling Missing/Lost Records

Lost records

- The member of staff should report the missing record to his/her supervisor/manager as soon as possible
- The supervisor/manager should ensure that a thorough search takes place, using tracking methods, including initiating a search at the base where the record should be kept
- The event must be entered in the Missing Record Log and in addition an Incident Form completed and forwarded to the Risk Manager
- A temporary record should be created, clearly marked as a temporary record, populated with all relevant information available for that data subject/individual. A temporary record should be set up and tracked on the relevant systems for the Department
- When original records are located the missing record log should be updated with details of where/how the original was located, and the two folders should be merged

Unavailable/Missing records

- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment
- An entry should be made in the Missing Records Log
- A temporary record should be created, as described in the above section
- If an appointment is deferred (i.e. individual has a meeting/appointment with HR) as the record is not available this should also be recorded in the Missing Record Log

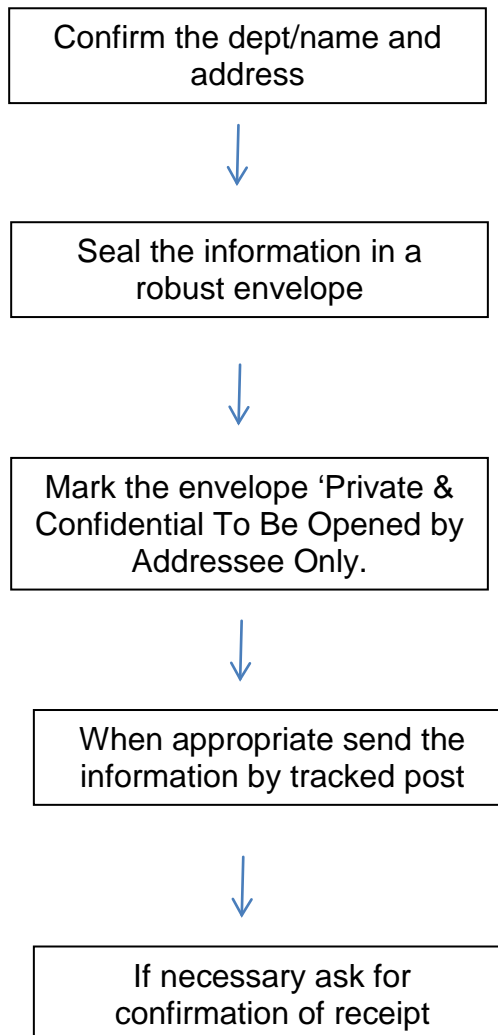
Reasons for records being unavailable may include:

- Record needed for another appointment/meeting
- Record with another Team/ Department
- Record not tracked
- Misfiled
- Wrong record/volume/temp record(s) sent

February 2018:	Page 30 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 5 – Sending Information via Postal Service

Guidance for sharing Personal, Confidential or Sensitive information by POST



Appendix 6 – Full Guidance on Retention Schedules

Full Guidance and retention schedules can be found here:

<https://digital.nhs.uk/codes-of-practice-handling-information>

February 2018:	Page 32 of 42	Records Management Policy:	Version No: 5.0
----------------	---------------	----------------------------	-----------------

Appendix 7 – Retention Schedule

Record Type	Retention start	Retention period	Action at end of retention period	Notes
9. Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings

Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Act. If records are not excluded by such an instrument they must either be transferred to a Place of Deposit as a public record or destroyed 20 years after the record has been closed.
--	--------------------------------------	----------	--	--

Record Type	Retention start	Retention period	Action at end of retention period	Notes
10. Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained

Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
11. Staff Records & Occupational Health				
Although pension information is routinely retained until 100 th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75 th birthday.				
Duty Roster	Close of financial year	6 years		Review and if no longer needed destroy
Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner		Review and if no longer needed destroy
Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday		Review and if no longer needed destroy
Occupational Health Report of Staff member under health surveillance where they have been	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer		Review and if no longer needed destroy

subject to radiation doses				
Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see the good practice box Staff Record Summary used by an organisation.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	

Appendix 8 – Classification Categories

Security Class/ Label	Unclassified Public	Security Class/ Label	CCG	Security Class/ Label	Customer Confidential	Security Class/ Label	CCG Confidential
Description	Public information relating to the CCG such as: <ul style="list-style-type: none"> - web pages, - Information in the public domain - policies - published papers, - press releases, - publicity, - Points of contact for the public 	Description	Data related to the CCG itself. This data is restricted to management approved internal access and protected from external access Examples include: <ul style="list-style-type: none"> - Standard operating procedures including all Security procedures - Data Flow maps - Information Asset Registers - Audits - Know-how & service level delivery plans - Costings and business proposals - In-house updates and news 	Description	Data from or identifying clients, public and patients in any form for processing by the CCG. Examples include: <ul style="list-style-type: none"> - All electronic transmissions from clients and patients and their representatives - All letters and hard copy documents from clients and patients 	Description	Data collected and processed by the CCG in the conduct of its business to employ staff to deliver services to clients and manage all aspects of corporate finance and strategic planning. Examples include: <ul style="list-style-type: none"> - Personal identifiable data including Personnel files, Investigations, and all 'Special Category/ sensitive' data as defined by the GDPR/DPA. - Salaries - Accounting data and financial reports that have not been approved for release. - Strategic data

							that has not been approved for release - Litigation related data - All electronic transmissions, documents, files and information marked as 'confidential'.
Storage	Stored on a centrally managed IT facility with back-up or appropriate third party storage	Storage	Stored on a centrally managed IT facility with back-up or appropriate third party storage	Storage	Stored on a centrally managed IT facility with back-up or appropriate third party storage with password protection and encryption Hard copy stored on site within secure locked storage Pen drives and unencrypted or	Storage	Stored on a centrally managed IT facility with back-up, password protection and encryption Hard copy stored on site within secure locked storage Pen drives and unencrypted or personal devices must not be used to access/store

					personal devices must not be used to access/store information		information
Dissemination, Access & Handling	<ul style="list-style-type: none"> - Widely available - unrestricted via dissemination & hard copy - Permission to modify/update restricted to authorised persons and following approved procedures 	Dissemination, Access & Handling	<ul style="list-style-type: none"> - Management approved access for staff or staff groups - Dissemination restricted to approved recipients via management approved channels - Hard copy only if part of approved process or management approval given - Permission to modify/update restricted to authorised persons via approved procedures 	Dissemination, Access & Handling	<ul style="list-style-type: none"> - Need for unambiguous consent for processing data - Management approved access for individual staff or staff groups - Dissemination prohibited except with management approval or as part of an approved processes - Original copy of correspondence must not be changed 	Dissemination, Access & Handling	<ul style="list-style-type: none"> - Need for unambiguous consent for processing data - Management approved access for individual staff or staff groups - Dissemination prohibited except with management approval or as part of an approved processes - Original copy of correspondence must not be changed

Sending & Sharing	Via web, email, hard copy or appropriate third party storage	Sending & Sharing	Internally shared on a needs-to-know basis Can be sent via NHS email, hard copy or via approved third party storage External sharing is only by express approval of the CCG management or as part of a management approved process.	Sending & Sharing	Need for unambiguous consent? Internally shared on a needs-to-know basis via NHS email, hard copy. External sharing is only by express approval of the CCG Management or as part of a management approved process via NHS email, registered post or Courier	Sending & Sharing	Internally shared on a needs-to-know basis via NHS mail or hard copy External sharing is only express approval of the CCG management or as part of a management approved process via NHS email, registered post or Courier
Security	Confidentiality: n/a Integrity: Low Availability: Low	Security	Confidentiality: Medium Integrity: High Availability: Medium	Security	Confidentiality: High Integrity: High Availability: High	Security	Confidentiality: High Integrity: High Availability: High
Example Security Measures	Can be stored on: - GMSS centrally managed IT facility - Service based IT folders and drives - Hard-copy file storage - Public facing web pages	Example Security Measures	Can be stored on: - GMSS centrally managed IT facility - Service-based IT folders and drives - Secure hard-copy file storage - Secure cloud storage	Example Security Measures	Must be stored on: - GMSS centrally managed IT facility - Secure password protected service based IT folders and drives - Regular back-up of data - regular review of need to keep data - Secure hard-copy file storage	Example Security Measures	Must be stored on: - GMSS centrally managed IT facility - Secure password protected service based IT folders and drives - Regular back-up of data - regular review of need to keep data - Secure hard-copy file storage

Disposal	Electronic data deleted using normal deletion processes available to all IT users Printed material disposed of via recycling waste	Disposal	Electronic data deleted using normal deletion processes available to all IT users Printed material disposed of via confidential waste bins.	Disposal	Electronic data deleted using secure IT approved deletion processes to ensure permanent deletion Printed material disposed of via secure waste bins.	Disposal	Electronic data deleted using secure IT approved deletion processes to ensure permanent deletion Printed material disposed of via secure waste bins.
-----------------	---	-----------------	--	-----------------	---	-----------------	---

Appendix 9 – Freedom of Information Act Exemptions

Category	Possible Exemption [sections(s) of the FOI Act]
Appointments	S 40 Personal information (may be subject to a public interest test)
Barred	S 44 Legal prohibitions on disclosure
Board	
Commercial	S 43 Commercial interests (subject to a public interest test)
Contracts	S 43 Commercial interests (public interest test)
For Publication	S 22 For future publication (public interest test)
Management	S 38 Endanger health and safety (public interest test)
Personal	S 40 Personal information (may be subject to public interest test)
Policy	S 22 For future publication (public interest test)
Proceedings	S 30 Investigations and proceedings S 31 Law enforcement