Records Management Policy

Version:	6.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Date ratified:	31 January 2022
Name of originator /author (s):	Bury CCG Interim Information Governance and Risk Strategic Advisor/DPO
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	February 2022
Review date:	January 2024
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Records Management Policy CCG.GOV.011.6.0
Category of Document in The Policy Schedule	Information Governance
Author(s) Contact(s) for further information about this document	GMSS IG Team CCG Interim Information Governance and Risk Strategic Advisor/DPO
This document should be read in conjunction with	All Information Governance Policies
This document has been developed in consultation with	NHS Bury CCG Information Governance Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place Knowsley Street Bury BL9 0SN Tel: 0161 762 1500
Copies of this document are available from	Bury CCG Corporate Office Bury CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury CCG Information Governance Operational Group	28th November 2013
1.1 = Policy once ratified	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	8th January 2014
2.1 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	10th December 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	15th February 2016
3.1 = policy once reviewed	GMSS IG Team	4th January 2018
4.0 = policy once ratified	NHS Bury CCG Information Governance Operational Group	30th January 2018
4.1 = review	NHS Bury CCG Information Governance Team	15th June 2021
5.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	18th June 2021
5.1 = policy once reviewed	NHS Bury CCG Information Governance Steering Group	31st January 2022
6.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	7th February 2022

Records Management Policy

Contents

1. Introduction and Aims

1.1. The purpose of this document is to provide guidance to all NHS Bury CCG (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.

1.3. The Records Management: NHS Code of Practice for Health and Social Care 2021 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 UK General Data Protection Regulation Protection (UK 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 aids compliance with UK 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 NHS 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 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; and
- reduced costs.

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 corporate function.

1.9. The development of these procedures and practices will help the organisation meet the required standards ensuring that records are managed and controlled appropriately throughout their life cycle, in the most cost effective way, and in accordance 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.

1.11. The aims of this policy are to ensure that:

- **Records are available when needed** - from which the CCG is able to form a reconstruction of activities or events that have taken place;
- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **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 and be badged with the CCG logo** – 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. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

2. Scope

2.1. This policy 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 applies to all third parties and others authorised to undertake work on behalf of the CCG.

2.2. This guidance relates to all clinical and non-clinical records held in any format by the CCG, or any party on behalf of 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;
- material intended for short term or transitory use, including notes and "spare copies" of documents;
- meeting papers, agendas, formal and meetings including notes taken by individuals in note books and bullet points are all subject to the above; and
- emails and other electronic communications.

2.3. The above list is not exhaustive.

- **Limitations and application for CCG staff**

2.4 The introduction of the Health and Social Care Act 2012 did not provide CCGs with the same powers and rights previously provided to Primary Care Trusts to obtain, handle, use and share confidential and identifiable information. In general, CCG staff are not entitled to use Personal Confidential Data (PCD). Whilst this policy 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.

2.5 Further information on the above is available in the latest CCG Staff IG Handbook and the Information Governance Policies.

3. Definitions

3.1. **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 sound, whilst at the same time serving the operational needs of the organisations 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.

3.2. 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.

3.3. In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity.' For working examples see below:

- **Corporate/business records**

3.4 These 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. 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
- Records in all electronic formats including emails

- **Health records**

3.5 These are 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.

3.4. **Information** is stored on records. The Records are important sources of administrative, evidential and historical information. They are vital to the organisation 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.

3.5. **Information Asset Register** lists forms of assets/ information/ files/ folders that are of value to the CCG.

4. Roles and Responsibilities

4.1. The following roles and responsibilities apply in respect to this policy:

- **Accountable Officer**

4.2 Overall accountability for records management across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

- **Caldicott Guardian**

4.3 The CCG Caldicott Guardian is the conscience of the organisation and are responsible for ensuring that national and local guidelines on the handling of confidential personal information are applied consistently across the organisation. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

- **Senior Information Risk Owner (SIRO)**

4.4 The CCG SIRO is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of information are in place. The SIRO is responsible to the Governing Body for ensuring that all Information risks are recorded and mitigated where applicable. The CCG SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

- **Information Asset Owners (IAOs) / Managers (IAMs) / Administrators (IAAs)**

4.5. Under the responsibility of the SIRO, Information Asset Owners 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 SAR;
- ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy, 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.

- **Data Protection Officer (DPO)**

4.6 The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the UK GDPR and other data protection laws. They are required to monitor compliance with

the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct 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.).

- **Information Governance Support Officer**

4.7. The CCG Information Governance Support Officer is responsible for co-ordinating, publicising, implementing and monitoring the records management processes and reporting issues or concerns to the Information Governance Steering Group.

- **Directors/Senior Managers/Information Asset Owners**

4.8. Directors, Senior managers and Information Asset Owners are responsible 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.

- **All Staff**

4.9 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.

4.10 It needs to be clearly understood by all employees and those authorised to work on behalf of the CCG, that under the Public Records Act 1958, they have a degree of responsibility for any record they create or use and may be subject to both legal and professional obligations.

4.11 Staff handling personal confidential information must remember they have a common law duty of confidentiality to patients and other employees and a duty to maintain professional ethical standards of confidentiality.

4.12 Managers will ensure that all staff have read this policy and understand the need for appropriate records management.

5. NHS Number

5.1. The NHS Number is 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 departments/services who have a legal basis to use NHS numbers will reference appropriately on all clinical communications, clinical records and on all systems processing patient information.

5.3. The CCG 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.

- **NHS Number Principals**

5.4. Find It

- Find / request the NHS Number on referral letters / forms received;
- Determine and verify the NHS Number before or 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.

5.5 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, documents and reports which include patient information and are used for that person's care;
- Ensure systems can support the NHS Number;
- Use the Personal Demographic Service (PDS) or Demographics Batch Service (DBS) to trace NHS Numbers.

5.6 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.

6. Registration of Record Collections

6.1. The CCG will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. The Information Asset Registers will facilitate:

- The classification of records into series; and
- The recording of the responsibility of the individuals creating records

7. Record Creation

7.1. The CCG should have a process for documenting its activities, taking into account the legislative and regulatory environment in which it operates.

7.2. 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.

7.3. 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.

7.4. 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 filling 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.

7.5. 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 filling systems to be documented and kept up to date.

7.6. Managers of departments should ensure staff are made aware of their responsibilities, are properly trained and that reviews and monitoring for compliance are undertaken.

7.7. 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.

7.8. 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:

- 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.
- For checklist on how to Create a Record refer to Appendix 1, Checklist; Creating a Record

8. Record Quality

8.1. 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.

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

8.3 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.

- **Quality Checking**

8.4 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:

- Eensure 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.

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

9. Record Keeping

9.1 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.

9.2. 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.

9.3. All records must conform to these record keeping guidelines, legislation, NHSLA, DoH, Information Governance requirements and professional guidelines.

10. Record Maintenance

10.1. 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.

10.2. 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.

10.3. 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.

10.4. 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.

10.5. 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.

10.6. 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.

10.7. Any duplicate documents (except where copy letters sent or received have had comments added by hand) should be culled and confidentially destroyed.

10.8. 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.

10.9. 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.

10.10. 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.

11. Tracking of Records

11.1. Accurate recording and knowledge of the whereabouts of all clinical and non-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.

11.2. 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).

11.3. 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.

11.4. Electronically operated tracking systems include:

- A computer database, excel spreadsheet in place of paper/card index;
- bar code labels and readers linked to computers;
- workflow software to electronically track documents.

11.5. 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.

11.6. 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;
- maintain a log of all records received into the department including the date received, service user name and NHS number.

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

12. Record Transportation

12.1. 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.

12.2. 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).

12.3. Off-site movement of records or other confidential/sensitive information

12.3.1 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. If a record is taken off site, it must be stored securely in accordance with the
- Confidentiality Code of Conduct – Guidelines for Staff;
- 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.

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

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

13. Lost/Missing Records

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

13.2. The loss of records constitutes a reportable incident and should be reported in accordance with the CCGs Incident Reporting Policy.

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

14. Scanning

14.1. 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).

14.2. 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.

15. Disclosure and Transfer of Records

15.1. 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 CCG's Information Governance Team prior to any disclosure. If the request for access to information is made under the Freedom of Information (FOI) Act 2000, then the request should immediately be forwarded to the Patient Services Department within the CCG in order to comply with the deadlines specified in the Act. This will be subsequently assigned to a competent member of staff at the CCG to handle.

15.2. 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.

15.3. 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 CCG's IG Team as well as GMSS IT Team can advise on appropriate safeguards.

16. Retention, Archiving and Disposal of Records

16.1. Appraisal of Records

16.2. 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.

16.3. 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.

16.4. 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.

16.5. 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.

17. Record Closure

17.1. 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 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.

17.2. 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.

18. Retention Schedules and Record Disposal

18.1. 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 the CCG's business functions.

18.2. The CCG has adopted the retention periods set out in the Records Management: NHS Code of Practice for Health and Social Care 2021. These retention schedules outline the recommended minimum retention period for NHS records.

18.3. Information Asset Owners, Information Asset Administrators and 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.

18.4. Where there are records held by the organisation that do not have a retention period advice should be sought from the Information Governance Steering Group where approval and inclusion of the retention period will be granted.

18.5. 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.

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

18.7. 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.

18.8. 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.

18.9. 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 GMSS IG Team.

18.10. It must be remembered that the destruction of records is an irreversible act.

18.11. Please see Appendix 7 – Data Deletion/Destruction Flow Chart, Appendix 8 – Request to Dispose of Information Form and Appendix 9 - Retention Schedule for further details.

19. Classification of NHS Information within the CCG

19.1. The aim of the Classification Marking of NHS Information is to demonstrate 'good practice' in marking the records for which the CCG are responsible.

19.2. This is applicable for information recorded on paper and that processed electronically including printouts, reports etc.

19.3. Through the application of this policy, the CCG will be able to further demonstrate the effectiveness of their local IG practices.

19.4. This policy should be considered alongside the following:

- NHS Codes of Practice and guidance on Confidentiality
- Information Security Management
- Acceptable Use Policy

19.5. This policy sets out a proposed simple scheme of classification relevant to the needs of the CCG

19.6. Please see Appendix 10 for details of the Classification Categories.

19.7. All staff working in the CCG are responsible for managing the documents and records they create or use in performance of their duties.

20. Freedom of Information

20.1. When classifying NHS documents regard should be paid to the requirements of the Freedom of Information Act 2000.

20.2. 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.

20.3. 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.

20.4 A note of the exemptions that might be relevant to the protective markings is included in

Appendix 11.

20.5. 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 team.

21. Training Requirements

21.1. A training needs analysis will be undertaken with staff affected by this document. Classification Marking of NHS Information

21.2. Based on the findings of that analysis appropriate training will be provided to staff as necessary.

22. Subject Access Request

22.1. A Subject Access Request, commonly referred to as a SAR, is a request from a data subject (individual) for a request 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 Subject Access Request (SAR).

22.2. Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless which media it is held in;
- have their information kept up to date;
- require the CCG 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.

22.3. In most cases the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent 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.

22.4. In most cases the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent 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.

22.5. 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.

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

23. Information Risk Management

23.1. Where required the information risk management process will take place in accordance with the CCGs Risk management Strategy. The CCG's 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 IG Steering Group and Audit Committee.

24. Records Management and System Audit

24.1. 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 (DPS Toolkit). The CCG will regularly audit its records management practices for compliance with the framework.

24.2. The audit will:

- Identify areas of operation that are covered by the CCG's 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.

24.3. The results of audits will be reported to the relevant quality and standards groups within the CCG under designated authority from the Audit Committee on behalf of the CCG Governing Body.

25. IG Training and Awareness

25.1. Information Governance training is required to be undertaken on an annual basis. CCG staff are mandated to undertake the mandatory Information Governance training annually. Records Management features in this training. All CCG Staff will be made aware of their responsibilities for record-keeping and record management.

25.2. Where staff may take on a specific Information Governance roles within the CCG i.e. Records Manager, additional Information Governance training will be required. For further guidance refer to the CCG Training Needs and Analysis (TNA) Document.

25.3. 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 IG Support Officer.

25.4. The CCG Information Governance Steering Group will be responsible for ensuring that this policy is implemented, and that the records management system and processes are developed, co-ordinated and monitored.

25.5. This policy will be placed on the CCG Intranet for all staff to access.

25.6. 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.

26. Monitoring and Review

26.1. This policy will be reviewed on a two yearly 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

26.2. Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

26.3. Equality Analysis Assessment

26.4. The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCG's legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

27. Legislation and Related Documents

27.1. All NHS records are public records under the Public Records Acts. 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 and Social Care 2021, in particular:

- The Public Records Act 1958;
- UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018;
- 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/.

27.2. This Policy should be read in conjunction with the following CCG Policies:

- Data Protections Policy
- Information Security Policy
- Email & Internet Policy
- Confidentiality Procedure
- Encryption Policy
- Acceptable Use of IT & Equipment Policy
- Secure Transfer Policy
- Information Risk Policy

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

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, EIA if applicable
- 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 invent of a claim or litigation

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.

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

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: ……

(inc postcode)……..

Method of transportation: ……..

Estimated duration of transit: …… ……..

Goods received by Courier/Organisation/Dept : 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/dept 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.

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:

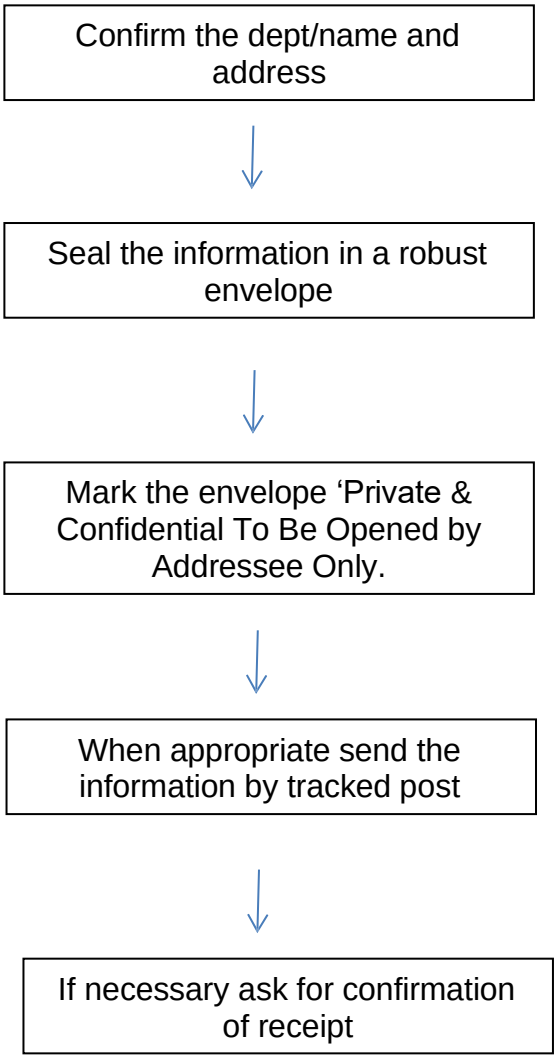
- A record is regarded as unavailable if it is in use elsewhere and/or cannot be retrieved in time for an appointment
- An entry should be made in the Missing Records Log
- A temporary record should be created, as described in the above section
- If an appointment is deferred (i.e. individual has a meeting/appointment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

Appendix 5 – Sending Information via Postal Service

Guidance for sharing Personal, Confidential or Sensitive information by POST

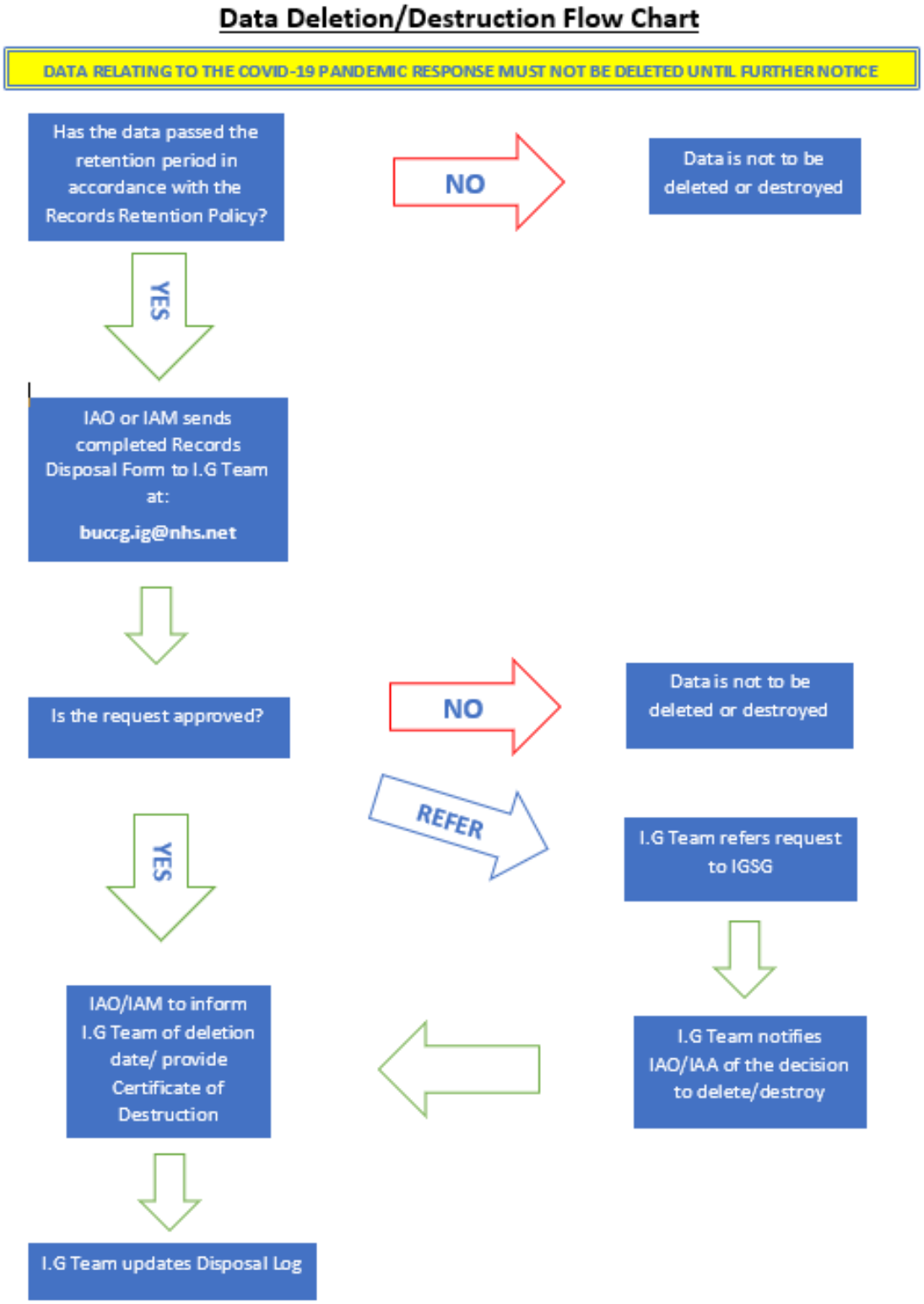


Appendix 6 – Full Guidance on Retention Schedules

Full Guidance and retention schedules can be found here:

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

Appendix 7 – Data Deletion/Destruction Flow Chart




KEY: IAO Information Asset Owner
IAM Information Asset Manager
IGSG Information Governance Steering Group
Records Retention Policy location:

Appendix 8 – Request to Dispose of Information Form

NHS
Bury
Clinical Commissioning Group

Request to Dispose of Information Form

Name of Service or Team:	
Name of person completing the form:	

Description of information or record to be destroyed/deleted	Number of records or number of lines of data to be destroyed/deleted	Information type	Full record or partial record destroyed?	Name of Information Asset Owner requesting the destruction/deletion	Date destruction/deletion approved by IGSG	Method of Disposal	Date of destruction/deletion	Additional Comments

NOTES:

* Please complete this form to request the deletion or destruction of official CCG electronic data or paper records because the retention deadline for the information has expired, according to the Records Management Policy.

* Please send your request to buccg.ig@nhs.net and do not destroy or delete any data until your request has been authorised by the IGSG.

* A central disposal log repository will be maintained by the I.G Team.

* If you have processed any data under the COPI arrangements for managing or planning purposes during the COVID-19 pandemic, please retain these records until advised otherwise.

Appendix 9 – 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. Consider transfer to PoD.	Includes minor meetings/projects and departmental business meetings These may have local historical value, so considered for archival interest.

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	Destruction certificates created by public bodies are not covered by a retention instrument; if they do not relate to patient care and if a PoD or The National Archives do not accession them, they need to be destroyed after 20 years.

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	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
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	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation, particularly where this resulted in changes to the services provided, and so

				may have historical value.
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.

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. Retention begins from the close of the financial year.
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 subject to radiation doses	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
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. Some PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the retention period has been reached.
Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy Review, and consider transfer to PoD	Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is ok to continue if this is

				what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to PoD. If the PoD does not require them, then they can be securely destroyed at this point.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy Retention begins from creation.	

Appendix 10 – 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: - 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: - 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: - 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: - Personal identifiable data including Personnel files, Investigations, and all 'Special Category/ sensitive' data as defined by the UK 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 personal devices must not be used to access/store information	**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 information

Dissemination, Access & Handling	- Widely available - unrestricted via dissemination & hard copy - Permission to modify/update restricted to authorised persons and following approved procedures	**Dissemination, Access & Handling**	- 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**	- 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**	- 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 11 – 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