PLEASE DESTROY ALL PREVIOUS VERSIONS OF THIS DOCUMENT

NHS
Islington
Clinical Commissioning Group

INFORMATION MANAGEMENT POLICY

1	POLICY DRAFTED BY:	NELCSU INFORMATION GOVERNANCE TEAM
2	ACCOUNTABLE DIRECTOR:	DIRECTOR OF QUALITY AND GOVERNANCE
3	APPLIES TO:	ISLINGTON CLINICAL COMMISSIONING GROUP STAFF
4	COMMITTEE & DATE APPROVED:	EMT 7th December 2016
5	VERSION:	1.0
6	RELATED DOCUMENTS:	CALENDAR, EMAIL AND INTERNET POLICY CONFIDENTIALITY AND DISCLOSURE OF INFORMATION POLICY INFORMATION GOVERNANCE FRAMEWORK AND STRATEGY INFORMATION GOVERNANCE POLICY INFORMATION SECURITY POLICY
7	DATE OF IMPLEMENTATION:	11/01/2017
8	DATE OF NEXT REVIEW:	OCTOBER 2018

DOCUMENT CONTROL

Date	Version	Action	Amendments
07/09/2016	1.0	New policy for Islington CCG in line with policies issued by NELCSU in accordance with SLA	

TABLE OF CONTENTS

1. Summary

Islington Clinical Commissioning Group (CCG) has put this policy in place to ensure staff are fully aware of their information management responsibilities. Information and records are an organisation's 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 organisation 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.

It is important to ensure information and records 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 original/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 reviewing and permanently preserving records with particular archival value.

The CCG is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law, statute and best practice. Compliance with all organisation policies is a condition of employment and a breach of policy may result in disciplinary action.

2. Scope

This policy covers all aspects of holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of the CCG.

This includes, but is not limited to; staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

This policy is applicable to:

- All records, information and data held and processed by the CCG. All information must be managed and held within a controlled environment. This includes personal data of patients and staff, patient level data (non-identifiable) as well as corporate information. It applies to records, information and data regardless of format, in addition to historic data held by the organisation;

- All permanent, contract or temporary personnel and all third parties who have access to premises, systems or information. Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual or voluntary basis;
- Information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed output from these systems, and
- All means of communicating information, both within and outside the CCG and both paper and electronic, including data and voice transmissions, emails, post, fax, voice and video conferencing.

2.1. Information Lifecycle Stages

The protocol applies to all stages of information and records management lifecycle, from the initial identification of a requirement through to its ultimate disposal:

Detailed information of the stages of the Information lifecycle is contained in in the Records Management Code of Practice Part 1 (2006).

2.2. Types of Information

The following is a list of information and systems within the scope of this protocol, the list is not exhaustive:

- Digital or hard copy patient health records (including GP medical records);
- Digital or hard copy administrative information (including, for example, personnel, estates, corporate planning, supplies ordering, financial and accounting records);
- Digital or printed X-rays, photographs, slides and imaging reports, outputs and images;
- Digital media (including, for example, data tapes, CD-ROMs, DVDs, USB disc drives, removable memory sticks, and other internal and external media compatible with NHS information systems);
- Computerised records, including those that are processed in networked, mobile or standalone systems;
- Portable communications devices such as mobile phones, Blackberry's, Personal Digital Assistant (PDA) I-pads, tablets etc.;
- Email, text and other message types;

3. Purpose

The Policy is intended to achieve and maintain the following Information Governance objectives:

Confidentiality

- assuring that sensitive information or data is accessible to only authorised individuals, and is not disclosed to unauthorised individuals or the public unless appropriate and lawful.

Integrity

- safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.

Availability

- ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

Accountability

- users will be aware of their responsibilities in relation to their collection, use and processing of data and information.

4. Roles and responsibilities

Role	Responsibilities
Governing Body	In line with the Guidance for NHS Boards: Information Governance, the Governing Body will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against following questions: 1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures, and are addressing the responsibilities and key actions required to support effective IG?" 2. "What were the outcomes of our most recent annual IG assessment, and what measures (if any) have been put in place to address any identified deficiencies?" 3. "What plans do we have in place to ensure our organisation remains compliant with national standards for IG? 4. "Do we as an organisation have the capacity and capability to guarantee our plans for IG can be implemented?" 5. "Do our IG arrangements adequately encompass all teams and work areas that we are legally accountable for?" 6. ''What plans do we have in place to ensure compliance with the Caldicott 2 recommendations?'' 7. ''What plans do we have for protected disclosures as a result of the Public Sector Information Regulations 2015?'' 8. ''Are all significant IG Risks being managed effectively and considered at an appropriate level? Have there been any serious incidents requiring investigation reported? ''
Accountable Officer	Has overall accountability and responsibility for governance within the organisation. Is to provide assurance that all risks to the organisation, including those relating to information, are effectively managed and mitigated.

Role	Responsibilities
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the IG agenda. • Fosters a culture for protecting and using data. • Ensures information risk requirements are included in the corporate Risk and Issue Management Policy. • Ensures Information Asset Owners (IAOs) undertake risk assessments of their assets. • Is responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Provides a focal point for the management, resolution and/or discussion of information risk issues. • Ensures that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff. • Ensures the Governing Body is adequately briefed on information risk issues. • Is accountable for information risk. The SIRO roles and responsibilities are defined in **Appendix 1 of the NHS Information Risk Management Guidance**. The role holder will be supported and advised by the IG Team.
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues.
Information Asset Owners	All senior staff at Director level are required to act as Information Asset Owners for the information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assists identified as within their remit. They will also: • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. The IAOs will be supported by IAAs who will ensure the above takes place. The detailed roles and responsibilities are defined in **Appendix 1 of the NHS Information Risk Management Guidance**
Information Asset Administrators	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how they work and how they are used. They will ensure there are procedures for using them, control access to them and understand their limitations. The detailed roles and responsibilities are defined in **Appendix 1 of the NHS Information Risk Management Guidance**
Information Governance Lead	Senior CCG Manager responsible for ensuring suitable advice, guidance support, tools and training are available to those with the CCG who handle data, to ensure they do so appropriately. This role will be the main point of contact for the NEL CSU IG Team.
NEL CSU IG Team	Provides specialist advice and support, under contract, to the organisation in relation to IG subject matters. They will also form part of the Caldicott function.

Role	Responsibilities
All Substantive/Permanent Staff	All those working for the CCG have legal obligations, under the Data Protection Act and common law of confidentiality; and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct to manage information appropriately. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.
CCG Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its functions. However it is recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.
Registered Healthcare Professionals	In addition to this policy any healthcare professional is under a duty to meet records management standards set by their professional regulatory bodies. Failure to do so may involve notifying the relevant body.

5. Policy Standards

This policy document, as part of a suite of supporting Information Governance related policies, sets out the standards that those working for or on behalf of the CCG are expected to adhere to when handling data or information.

5.1. Accountability and Governance

The CCG will put in place suitable controls to:

- Assign responsibilities to oversee the delivery of standards set out in this policy
- Report on compliance against Information Governance to a suitable committee within the organisation
- Ensure that all staff have been made aware of their responsibilities, how to comply with them and have available advice and guidance and training programmes to do so
- Ensuring the consistency of information governance across the organisation;
- Develop information governance policies and procedures;
- Ensuring compliance with Data Protection, and other information security related legislation;
- Providing support to the team who handle freedom of information requests;
- Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO).

5.2. Definition of a Record

The definition of a record is documentary evidence, regardless of form or medium, created, received, maintained and used by the organisation in pursuance of its legal obligations or in the transaction of business.

This definition draws a distinction between a record and a document – a record is a final version that may be retained, while a document can be changed and will not normally be retained, except for audit trail purposes where necessary. The purpose of a record is to preserve information in a form that is trustworthy and, once declared, should not be changed.

A record is only created when there is a need to remember the details of an event, decision or action. Creation is supported by a process of lodging a document into a record keeping system; including the

registration and classification of the record, and assigning metadata to describe the record and place it in context.

> The life of a record runs from its creation/receipt through the period of its 'active' use, into a period of 'inactive' retention (such as closed files which may still be referred to occasionally), and finally onto either preservation or confidential destruction.

5.3. Personal Confidential Data

Personal Confidential Data (PCD) relates to information about patients, service users and members of staff and can include anything that makes them identifiable. It does not have to include particular demographic information, such as name and address, and can consist of a combination of factors that would make it possible to identify the individual.

Information provided to the NHS is done so on the expectation of confidence and often in a healthcare setting. It is important for staff and working practice to account for this and to ensure that any secondary use of personal data, for non-care purposes, is done in accordance with legal, regulatory and organisational requirements.

The organisation will provide and maintain a privacy notice, or fair processing notice that details what personal data is held and processed, for what purpose it is processed, who it is shared with and what governs that process.

5.4. Data/Information Classification

Information assets were previously classified and marked using the adapted NHS national classification scheme. All information assets should be classified and marked according to the following terms.

Marking	Description
NHS Confidential	This is appropriate for documents and files containing person-identifiable clinical or staff information given in confidence not for general disclosure. Access should be tightly controlled and restricted.
NHS Protect or Restricted	This applies to corporate records where the basic principles would be to handle with care, restrict disclosure and secure.
NHS Public	Any information which does not warrant being marked with one of the above classifications is to be marked NHS Public. These records should be considered to be open and routinely made available to the public.

With effect from April 2014, new Government Security markings have been introduced to replace these markings. This does not apply retrospectively.

Marking	Description
NHS Official	All routine CCG business, operations and services should be treated as OFFICIAL. The subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL should be used where applicable. Ordinarily NHS Official information does not need to be marked.

NHS Official-Sensitive	This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
NHS Official-Sensitive: Commercial	Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG, other NHS body or a commercial partner if improperly accessed.
NHS Official-Sensitive: Personal	Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Where existing information is marked NHS Confidential it should be treated as NHS Official: Sensitive

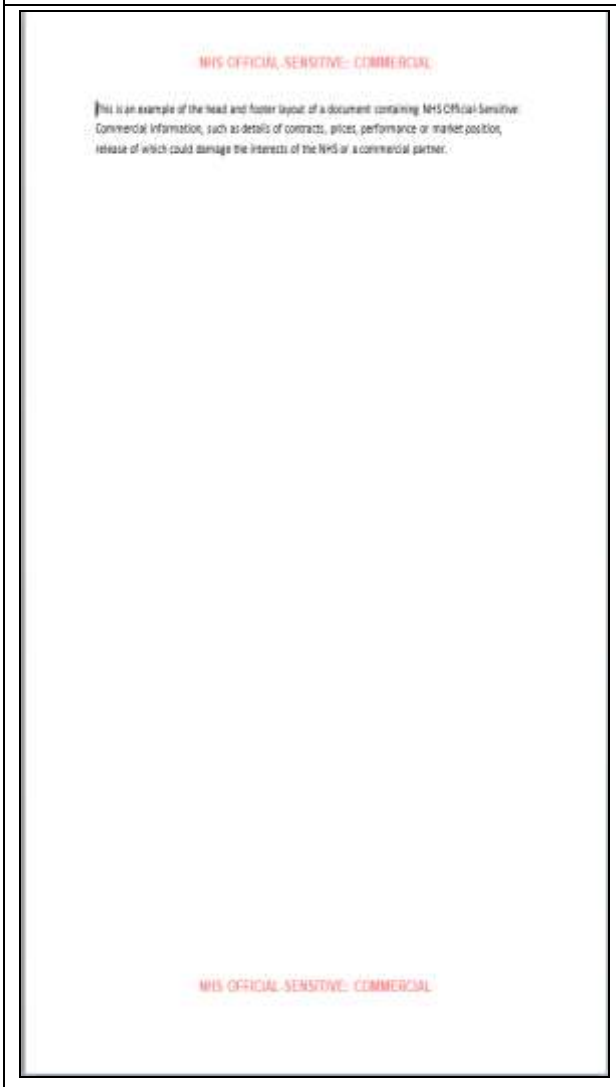
NHS Official-Sensitive (including NHS Official – Sensitive: Commercial and NHS Official – Sensitive: Personal) information should be secured using the standards set out in this policy for as long as they are held until securely disposed of.

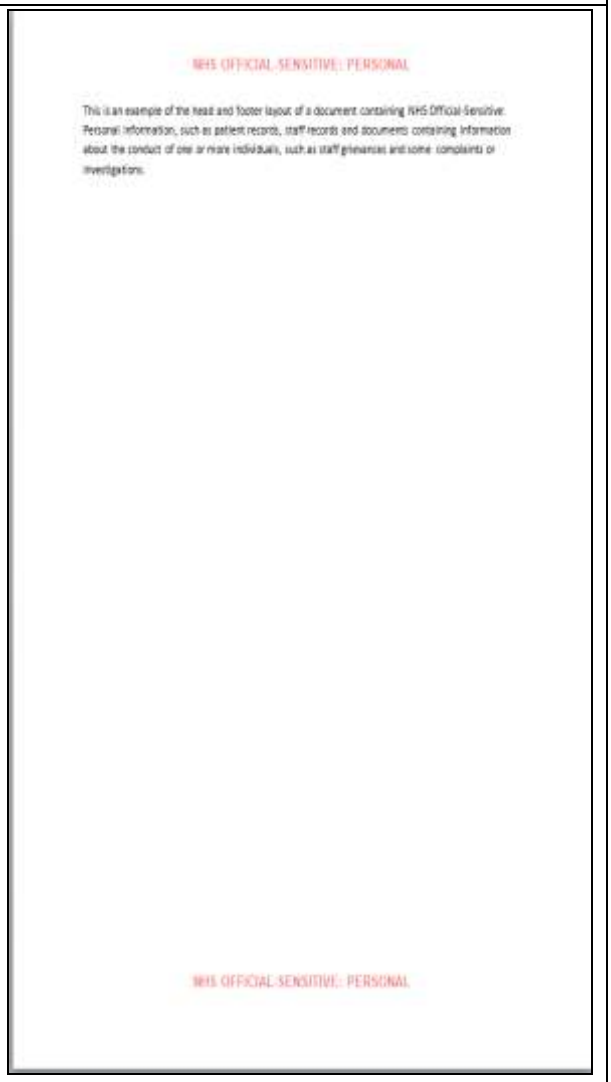
How to handle and store OFFICIAL information:

EVERYONE is responsible to handle OFFICIAL information with care by:

- Applying clear desk policy
- Sharing information with the right people
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

Examples of the use of the markings are shown below:


NHS OFFICIAL SENSITIVE: COMMERCIAL
This is an example of the head and footer layout of a document containing NHS Official-Sensitive: Commercial information, such as details of contracts, prices, performance or market position, release of which could damage the interests of the NHS or a commercial partner.
NHS OFFICIAL SENSITIVE: COMMERCIAL


NHS OFFICIAL SENSITIVE: PERSONAL
This is an example of the head and footer layout of a document containing NHS Official-Sensitive: Personal information, such as patient records, staff records and documents containing information about the conduct of one or more individuals, such as staff grievances and some complaints or investigations.
NHS OFFICIAL SENSITIVE: PERSONAL

5.5. Information Quality

The CCG recognises the importance of quality information to make informed decisions. As such the CCG will ensure processes are in place to maintain the quality of information as outlined within the data quality section of this policy.

6. Information Management (Records Management)

The CCG will be required to maintain records of its own activity. The CSU also maintains records on behalf of the CCG. The CCG will ensure it implements robust management of information to enable the organisation to reduce costs, improve efficiency and enhance the ability to monitor the performance of contracts and commissioned services.

Each IAO will be required to have records management systems in place within departments to securely take information from creation and use all the way through to retention for appropriate periods to disposal (secure destruction or permanent preservation) as outlined in the diagram below.

Figure 1[i]

6.1. Information Management System Design

One of the key elements of Information management throughout the lifecycle of information is the design of systems to capture information and records.

It is important that the procurement, commissioning or system design process completes a thorough analysis.

6.2. Creation

Record creation is one of the most important processes in records management and should be captured or filed into a filing system to suit the specific service. Each service should develop a process that ensures:

- Records are held on a media that will be durable and last until its specified retention period.
  - Manual records should have secure fastening e.g. treasury, ring binders etc.
- A clear filing and naming structure with instructions for the location of documents in each section. Furthermore, they should be held in order, which together will facilitate easy entry and retrieval of information.

- The application of a unique reference to all records; these should be relevant to the type of record they are. For example, but not limited to:
    - Staff Assignment number for human resource records
    - NHS Number for health records unless not possible
    - Unique reference for corporate records as determined by the departmental area.
- Records are kept in their context, are classified using the Government security scheme, and are stored securely relative to the marking applied.
- A tracking and tracing system is used within each department/service which enables the movement and location of records to be controlled and provide an auditable trail of record movement. Systems may vary depending on operational need but should include:
    - The item reference number or identifier;
    - A description of the item (for example the file title);
    - The person, position or operational area having possession of the item;
    - The date of movement.

6.3. Saving on Shared Folders, Desktop and Personal Folders

The vast majority of electronic information created as part of your job role should be stored in shared folders on the 'BLUE' network.

The reasons for this are:

- All information created by you as part of your work constitutes a record /evidence of the CCG's activity and may be needed for reference by others in future
- Easier to share information with other colleagues
- All records have a set retention period, similar files kept together are easier to retain for appropriate timescales
- Avoids duplication in storage of information
- Reduces confusion, easier to locate the master/original document
- Reduces the need to email documents to colleagues in the same directorate
- Information must be accessible if an individual leaves the CCG or is unexpectedly absent
- Able to locate information to comply with requests for information under the Freedom of Information Act, Data Protection Act or the Environmental Information Regulations.

Folders may also be created on the 'BLUE' network where access needs to be restricted, due to the sensitivity of the contents. The creation of such folders needs to be authorised by the owner (Information Asset Owner) of the folder.

Desktop / Personal folder

Staff must not store any CCG documents, records, or information on the desktop or in your personal folder.

This is due to the fact that information stored in these places is not backed up, so if the computer crashes, this information is lost. Information stored on the C: Drive (hard drive of the computer) is neither confidential nor secure.

The exception to this is shortcuts to folders or documents which can be stored on the desktop.

Ideally, person sensitive data should not be stored on any removable media, however if there is no other option ensure this data is stored on a corporate encrypted device and deleted once transferred to an identified secure area folder.

6.4. Working from home

All person identifiable data or commercially sensitive data must be saved with appropriate security measures. A secure drive CCG Network drive has been created to hold such data and this is linked to the Username of the individual. There is also the Blue Network Drive (letter) to save information but this may be also available to other team members. If staff are in doubt then they need to contact the IT Helpdesk.

Staff should not use home email accounts or private computers to hold or store any sensitive records or information which relates to the business activities of the CCG

When printing paper records, especially sensitive documents, ensure appropriate measures have been taken in collecting all documents immediately after printing.

6.5. Use of Records

Within each service the use of records will vary dependant on the nature of the service and the purpose of the record, however some key policy requirements are established below.

Original Records

The use of any original records within the service should be controlled, and only those authorised to make additions, alterations or close/finalise records should be able to do so. For example, when a draft policy is approved, or written originals are held.

Finalised Corporate Documents

The use and distribution of finalised corporate records should be controlled in line with the Government security marking scheme and read only copies be made available. The original must be kept by owner of the document. Only the original document and its versions are the corporate record.

Copies of Records

Any record that is copied or printed from an electronic or manual record should be marked as such as it is not the original record. It should be given the same security provisions and restrictions on disclosure as the original record.

If a copy of a record is altered or annotated in any way it then becomes a new record, and must follow its own records lifecycle.

Duplicate Records

Where multiple copies of the same record exist the master copy should be identified, along with the owner, where it is stored and any changes or additions should be made to the master copy.

6.6. Maintenance

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in the format.

Scanning

An important element in meeting the requirement for accessibility and completeness of records is considering which records should be scanned. This is a process that will be addressed on a case by case basis given the expenses involved. Any scanning will ensure that it follows clear systems and processes to maintain its legal admissibility and allow any manual records to be destroyed after validation.

6.7. Disposal

Disposal is defined as the management intent for a record once it is no longer required for the conduct of current business. Data and information not classified as a record may be destroyed once its business value is concluded.

There are a number of stages in the disposal phase of a corporate record which will be outlined in supporting Records Management guidance. These include:

Closure

Records are made inactive, such as approved versions of minutes or policies, or a previous version is replaced.

Retention

Once a document is no longer in use or active, it must then be stored for an appropriate period. The CCG will follow the DH Records Management Code of Practice regarding retention periods which specifies how long each type of record has to be kept placed within supporting guidance. Locally agreed retention periods will be established when necessary taking into account relevant best practice and prevailing legislation.

Additional retention

Under limited circumstances it may be decided that an individual's record, or specific type of record may need to be kept for longer than specified within retention periods. Decisions to extend retention periods must be clearly documented, an understandable rationale provided and new retention period established.

Archiving

Where appropriate information will be transferred to secondary storage areas to maximise use of space and maintain the security and integrity of the required data. All information transferred to archiving

should only be done after consultation with the CCG internal IG lead or CSU IG Team and be clearly logged in line with any issued guidance.

National Archives – The National Archives is a centre of expertise in creating, managing and preserving official information and is the UK government's official archive. They give detailed guidance to government departments and the public sector, including the NHS, on information management and advise others about the care of historical archives.

Any records that have historical value to the CCG will be kept and sent to the National Archives, where it will be kept for the future of the organisation and may never be destroyed. This is the final phase of a records lifecycle.

The CCC will need to identify its place of deposit and then transfer those records identified.

Destruction of Records

Once a record has reached its retention period, and it has been appraised as no longer being required it can be destroyed and this is an irreversible act. As many records contain sensitive and/or confidential information and their destruction must be undertaken securely. The method of record destruction must meet the standards set out within the Information Security Policy to provide adequate safeguards against the accidental loss or disclosure of the contents of the records.

When destroying records the following must be done:

- A list of records being destroyed must be kept. This should show their reference, description and date of destruction. (Disposal schedules would constitute the basis of such a record.)
- Certification should be received and kept as proof of destruction
- If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.
- At no time should records be left unsecured whilst awaiting destruction

7. Data Quality

The CCG recognises that reliable and accurate information is a fundamental requirement to manage personal or corporate information. In the new commissioning landscape it will be important to have high quality data to generate useful information to ensure the effective commissioning and contract monitoring of services.

A fundamental principle of data quality is that data should be right first time, which means that the responsibility for getting the data right is at the point at which it is recorded.

Services should identify any barriers to good data quality; these may be cultural, process related, knowledge/skills based, or system based. Poor data quality should be seen as a risk and recorded by each IAO where identified and placed on the corporate risk register.

7.1. National Standards

The CCG will ensure that it and commissioned services manage data in line with National Standards such as the Information Standards Notices (ISN) and the Information Governance toolkit.

7.2. The Elements of Data Quality

The aim of any data quality exercise is to ensure that data is fit for purpose.

- Accessibility - Information can be accessed quickly and efficiently through the use of systematic and constituent filing
- Accuracy – information is accurate, with systems that support this work through guidance
- Completeness – the relevant information required is identified and working practice ensures it is routinely captured
- Relevance – information is kept relevant to the issues rather than for convenience with appropriate management and structure
- Reliability - Information must reflect a stable, systematic and consistent approach to collection, management and use.
- Timeliness – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently
- Validity - Information must be collected, recorded and used to the standard set by relevant requirements

8. Security of Records

Throughout the Information Lifecycle records should be kept secure, in line with the Information Security Policy, and only accessed by appropriate persons. The level of security will depend on the protective marking/classification of documents.

NHS Official-Sensitive (including NHS Official – Sensitive: **Commercial and NHS Official – Sensitive: Personal)** should be secure at all stages of the Records Lifecycle.

To do this the following should be in place:

- Access and disclosure should be properly controlled in line with the tracking and tracing requirements
- Records should be secure from unauthorised or inadvertent access or alterations. Audit trails must be in place to track the use and changes
- Assignment of responsibilities to protect records from loss or damage over time.
- The accommodation should also have proper environmental controls and adequate protection against fire and flood.
- Records should be stored in a secure location when not in use, e.g. lockable filing cabinets/cupboards, rooms locked and/or alarmed when out of normal working hours.
- NHS Official-Sensitive (including NHS Official – Sensitive: Commercial and NHS Official – Sensitive: Personal) should only be disclosed if it is lawful and is secure i.e. meets Information Security Policy and supplementary guidance.
- When using another organisation to archive records it is essential an agreement/contract is in place detailing how the records will be archived and who will be allowed access, details of the person and the reason access was required.
- If records are taken away from the archive a tracking system should be in place to identify who has taken the records and should be recorded when the record is returned to storage.

- Ensuring that records are transported in a secure and confidential manner. Whoever transports the records from one site to another should be contractually bound to comply with the necessary requirements and follow best practice and or any issued IG guidance
- It is the responsibility of the staff member who is leaving their current post or the organisation, and their Line Manager, to identify as part of the exit procedure specific records that should be retained in line with Department of Health Record Retention Schedule. These records should then be transferred securely to the CCG network drive and any non-work related records disposed of safely and securely.

9. Publication and Requests for Information

A number of legislative requirements place an obligation for information to be provided upon request. This policy commits the organisation to ensure that they comply with such requirements under the

- Freedom of Information Policy – Routine publication of information and response to requests for corporate information held by a public authority.
- Data Protection Act 1998– Subject Access Requests
- Access to Health Records Act 1990

10. Records as Information Assets

In line with the Information Security Policy, all information will be seen as an asset and require registration and assessment of appropriate risks. Directors will be required to ensure each service maintains the information asset register to include stores of clinical and corporate records.

For more information see the Information Security Policy and supporting guidance.

11. Records Management Incidents

The permanent or temporary loss or unavailability of a record or records should be seen as an incident, in line with the Information Security Policy and reported.

12. Support and guidance

The CCG will provide guidance documents to supplement this policy as necessary to provide staff with clear expectations in relation to expected records management practices. These should be seen as an extension of this policy.

13. Training

All staff are, as a minimum, mandated to undertake the “Introduction to Information Governance” e-learning module once followed by the “Information Governance Refresher” on an annual basis.

There is additional online annual IG training for Information Asset Owners (IAO), Information Asset Administrators (IAA), Senior Information Risk Owner (SIRO) and Caldicott Guardian (CG). For further details of this training refer to the Information Governance Policy or contact your local CCG IG lead/CSU IG Team.

14. Relationship with Service Providers

As a commissioner of clinical and support services the CCG will ensure that any organisations from which it buys services meets expected IG standards.

14.1. Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract in place to form a joint data controller relationship regarding the information required to effectively monitor commissioned services.
- Services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office.
- Complete the annual Information Governance Toolkit and undertake an independent audit/service review, to be disclosed to the CCG on request, in order to provide assurance they have met expected requirements.
- Ensure privacy notices make individuals aware of a CCGs role in commissioning and the personal and sensitive data it may receive to undertake such a role.
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract.
- Ensure there is consideration including process and identification of funding to ensure the continued management of information for the relevant retention of said information at the end of the contract.

14.2. Support services

All support services that process information on behalf of the CCG will be required to ensure:

- A suitable contract is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG.
- The services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing, maintaining a registration with the Information Commissioners Office
- Complete the annual Information Governance Toolkit and undertake an independent audit, to be disclosed to the CCG on request, in order to provide assurance they have met expected requirements.
- That any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity.
- Report any known incidents or risks in relation to the use or management of information owned by the CCG.
- Ensure there is consideration including process and identification of funding to ensure the continued management of information for the relevant retention of said information at the end of the contract.

15. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected 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 protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

The equality impact assessment has been completed and has identified impact or potential impact as "minimal impact".

16. Dissemination and Implementation

This policy will be made available to all relevant stakeholders via the CCG internet site. Additionally they will be made aware via email and this policy will be included for reference where necessary.

The policy will be supported by additional related policies and resources to support implementation. This will include the availability of, and access to, written and verbal advice, guidance and procedures where necessary.

17. Non-conformance with this Policy

Should it not possible to meet the requirements within this policy and associated guidelines this must be brought to the attention of the department's Information Asset Owner. Any issues will need to be documented as a risk and either:

- Accepted and reviewed in line with this policy
- Accepted with a view to implementing an action plan to reduce the risk
- Not accepted and the practice will stop until such time as the risk can be reduced

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

18. Monitoring and Review

Performance against the policy will be monitored against

- Availability and dissemination of policy, in alternative formats where requested or need identified
- Acceptance and understanding of audience (training, spot checks, surveys)
- Reports of non-conformance i.e. incidents or risks
- Compliance against the Information Governance Toolkit

This policy will be reviewed every 2 years and in accordance with the following on an as and when required basis:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;

- Identified deficiencies, risks or following significant incidents reported;
- Changes to organisational infrastructure.

Appendices

Appendix A. Equality and Equity Impact Assessment

This is a checklist to ensure relevant equality and equity aspects of proposals have been addressed either in the main body of the document or in a separate equality & equity impact assessment (EEIA)/ equality analysis. It is not a substitute for an EEIA which is required unless it can be shown that a proposal has no capacity to influence equality. The checklist is to enable the policy lead and the relevant committee to see whether an EEIA is required and to give assurance that the proposals will be legal, fair and equitable.

The word proposal is a generic term for any policy, procedure or strategy that requires assessment.

	Challenge questions	**Yes/ No**	**What positive or negative impact do you assess there may be?**
1.	Does the proposal affect one group more or less favourably than another on the basis of:	No	
	▪ Race		
	▪ Ethnic origin (including gypsies and travellers, refugees & asylum seekers)		
	▪ Nationality		
	▪ Gender		
	▪ Culture		
	▪ Religion or belief		
	▪ Sexual orientation (including lesbian, gay bisexual and transgender people)		
	▪ Age		
	▪ Disability (including learning disabilities, physical disability, sensory impairment and mental health problems)		
2.	Will the proposal have an impact on lifestyle? (e.g. diet and nutrition, exercise, physical activity, substance use, risk taking behaviour, education and learning)	No	
3.	Will the proposal have an impact on social environment? (e.g. social status, employment (whether paid or not), social/family support, stress, income)	No	
4.	Will the proposal have an impact on physical environment? (e.g. living conditions, working conditions, pollution or climate change, accidental injury, public safety, transmission of infectious disease)	No	
5.	Will the proposal affect access to or experience of services? (e.g. Health Care, Transport, Social Services, Housing Services, Education)	No	

An answer of 'Yes' to any of the above question will require the Policy lead to undertake a full Equality & Equity Impact Assessment (EEIA) and to submit the assessment for review when the policy is being approved.

Appendix B. Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	The Information Governance Review, Mar 2013 (Gateway Ref:2900774) pg. 125
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	The Information Governance Review, Mar 2013 (Gateway Ref:2900774) pg. 125
Personal Identifiable Data or PID	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	The Information Governance Review, Mar 2013 (Gateway Ref:2900774) pg 125
Personal Confidential Data or PCD	This is information about a person which would enable the person's identity to be established. This can be explicit such as the name and address or different items together which combined could reasonably be considered to identify the individual.	
Sensitive Personal Information	There is a precise definition of sensitive information within the Data Protection Act 1998 for Personal Data. It includes information about the health of an individual; within the NHS it is safe to assume that most information about patients can be considered sensitive if it includes any details of health conditions or treatment. For more information see the Data Protection Protocol	DPA 1998
Sensitive Information	This is information such as financial or security information that should be considered sensitive. Access to this information needs to be controlled and restricted to specific post holders.	Government Security Classifications April 2014

Term	Definition	Source
Safe Haven	A ”Safe Haven” is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves, or is transmitted within the organisation by any means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven protocol and relevant procedure.	
Records Management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records’.	ISO 15489
Record	Documentary evidence, regardless of form or medium, created, received, maintained and used by the Cluster in pursuance of its legal obligations or in the transaction of business. This definition draws a distinction between a record and a document – a record is a final version that may be retained, while a document can be changed and will not normally be retained except for audit trail purposes where necessary. The purpose of a record is to preserve information in a form that is trustworthy and, once declared, should not be changed.	
Records Life Cycle	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 preservation or confidential destruction.	
Information Security	Securing, safeguarding and protecting the confidentiality, integrity and availability of all information, electronic or otherwise’	
Clinical Records	Consists of any information relating to the physical or mental condition of an individual and/or has been made by or on behalf of a health professional in connection with the care of that individual. This is regardless of format.	
Corporate Records	Records (other than clinical records) that are of, or relating to, an organisation’s business activities covering all the functions, processes, activities and transactions of the organisation and of its employees. A document becomes a record when it has been finalised and become part of the organisation’s corporate information.	
Protective Marking	Records should be marked to signify the nature of the contents and the level of security that should be applied to them.	
Destruction	The process of eliminating or deleting records beyond any possible reconstruction	ISO 15489

Term	Definition	Source
Disposal	The implementation of appraisal and review decisions for the destruction, permanent preservation of records or the movement of records from one system to another (for example, paper to electronic)	

Appendix C. Evaluation

Monitoring requirements 'What in this document do we have to monitor'	The management of information risks (Information Risk Management) Compliance with the law Compliance with the Information Governance Toolkit Incidents related to the breach of this policy
Monitoring Method	Information Risks will be monitored through the Risk Register and management system. Compliance with law will be monitored through audit, work directed by the Information Governance Toolkit and as directed by the SIRO The Information Governance Toolkit will be monitored by assessment of evidence against the objective of the relevant requirement. In addition, the IGT will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements
Monitoring prepared by	The CSU Information Governance Team and the CCG IG Lead for the relevant groups Incident reports will be produced by the nominated investigation officer
Monitoring presented to	Relevant CCG committees or groups with oversight of Information Governance Senior Information Risk Owner Caldicott Guardian
Frequency of Review	Yearly updates will be provided to the relevant groups, the SIRO and the CG Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Board will be provided. The internal audit report on IGT performance will be provided to the Board or delegated sub-committee. Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident