NHS
Wakefield
Clinical Commissioning Group

Records Management and Information Lifecycle Policy and Procedures

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Operating Officer / SIRO
Clinical Lead:	Caldicott Guardian
Author:	Senior Information Governance Officer & Information Governance Manager
Date Approved:	16th January 2020
Committee:	Integrated Governance Committee
Version:	5.0
Review Date:	April 2020

Version History

Version	Date	Author	Status	Comment
1.0	December 2014	IG Associate /Governance & Board Secretary	Approved	Policy approved by Integrated Governance Committee on 18 December 2014
2.0	December 2016	Senior IG Officer & IG Manager	Approved	Added to Skyline
2.1	May 2017	Governance & Board Secretary	Approved	Amendments to reflect new role of Associate Director of Corporate Affairs
2.2	January 2018	Information Governance Manager	Approved	Amendment to policy to reflect a revised next review date, as agreed by the IGC in December 2017
2.3	Feb 2018	Information Governance Manager	Draft	Review of policy and associated procedures. Amendments to reflect changes under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017).
2.4	April 2018	Information Governance	Draft	Policy approved by IGC subject to minor

		Manager		amendments to remove names and job titles of key IG related roles detailed within the policy and associated procedure. Reference to IG Policy and Framework organisational chart.
3.0	April 2018	Information Governance Manager	Approved	Approved by IGC April 2018
3.1	October 2018	Information Governance Manager	Approved	Minor amendments suggested to reflect adoption of a local Records Retention Schedule
3.2	December 2018	Information Governance Manager	Draft	Amended to comply with new Data Security and Protection Toolkit requirements
4.0	January 2019	Information Governance Manager	Approved	Approved by IGC January 2019
4.1	November 2019	Information Governance Manager	Draft	Minor amendment to Appendix J 'Subject Access Request and Access to Health Records Procedure' to reflect that Subject Access Requests can be made verbally as well as in writing.
5.0	January 2020	Information Governance Manager	Approved	Approved by IGC January 2020

Contents **Page**

Glossary of Terms

'Data Subject'	A natural person whose personal data is processed by a controller or processor.
'Health Record'	Information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual.
'Personal Data'	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
'Record'	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (the ISO standard, ISO 15489-1:2016 Information and documentation - records management).
'Records Management'	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.
'Subject Access Right'	Entitles the data subject to have access to and information about the personal data that a controller has concerning them. Also known as the Right of Access.

1.0 Introduction

1.1 NHS Wakefield Clinical Commissioning Group (CCG) recognises the importance of reliable information in terms of the efficient management of services and resources. The CCG also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which it creates, processes, stores, shares and disposes of information.

1.2 The Records Management and Information Lifecycle Policy and Procedures set out the CCG's overall approach to the management of records and should be read in conjunction with the other information governance policies and procedures detailed in Section 26.

1.3 NHS Wakefield Clinical Commissioning Group's records are the corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the CCG, its clients and the rights of NHS staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.4 It is the responsibility of all staff and governing body members including those working on behalf of NHS Wakefield Clinical Commissioning Group (CCG), those on temporary or honorary contracts, agency staff and students to comply with this policy.

1.5 Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate professional regulatory body, health and care regulator as well as the police.

2.0 Scope

2.1 This policy relates to all records held in any format by the CCG.

2.2 Examples of records which have been created or collated as a result of the work of the CCG include: -

- Patient information and health records (electronic or paper based)
- Administrative records (including e.g. personnel, estates, financial and accounting records: notes associated with complaint-handling)
- Photographs, Microform (i.e. fiche/film) Audio and videotapes, cassettes, CD-ROM, digital images and other images
- Computer databases, output, and disks etc, and all other electronic records
- Material intended for short term or transitory use, including notes and 'spare copies' of documents
- Meeting papers, agendas, records of formal and informal meetings including notes taken by individuals in note books and bullet points are all subject to the above

- Emails and text messages.

2.3 If any aspect of records management is contracted to another organisation the service provider must comply with the requirements of this policy.

2.4 Partner organisations providing support services to the CCG such as providers of commissioned services and 3rd parties that have access to our records will be expected to manage CCG owned records in accordance with this policy.

3.0 Aims

3.1 The aim of this policy is to ensure that all staff understand their obligations with regard to any records which they come into contact with in the course of their work and to provide assurance to the Governing Body that such information is dealt with legally, securely, efficiently and effectively.

This will 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** – 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 (see **Appendix F**), 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.

- **the CCG complies with the law and professional guidance**

4.0 Accountability

4.1 The Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available for the effective implementation of this policy and to receive by exception, significant risks and gaps in compliance on issues relating to records management.

4.2 Accountable Officer

The Chief Officer is the Accountable Officer of the CCG and has overall accountability for Records Management. The Chief Officer is required to provide assurance, through the Annual Statement of Internal Control that all risks to the CCG, including those relating to records are effectively managed and mitigated.

4.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of risk associated with records management including the responsibility for ensuring the CCG has appropriate systems and policies in place to effectively manage information risk. The SIRO is expected to be a voting member on the Governing Body. For details of the name and job title of the SIRO, please see the Information Governance Management Framework organisational chart within Appendix A of the IG Policy and Framework.

4.4 Caldicott Guardian

The Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared and disclosed in an appropriate and secure manner. The Caldicott Guardian is advisory. The Caldicott Guardian is expected to be a voting member on the Governing Body. For details of the name and job title of the Caldicott Guardian, please see the Information Governance Management Framework organisational chart within Appendix A of the IG Policy and Framework.

4.5 Data Protection Officer

The Data Protection Officer (DPO) is responsible for the provision of advice on compliance obligations, data protection impact assessment and monitoring of data protection compliance in respect of records management and the right of access by data subjects. For details of the name and job title of the DPO, please see the Information Governance Management Framework organisational chart within Appendix A of the IG Policy and Framework.

4.6 Information Governance Lead

The Information Governance Lead (Governance and Board Secretary), supported by the Information Governance Team, is responsible for co-ordinating, publicising, implementing and monitoring compliance with the records management policy.

4.7 **Information Asset Owners and Administrators**

Information Asset Owners (IAO) are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets/records that they are responsible for and that any new business processes or changes introduced to their business processes and systems undergo a data protection impact assessment.

Information Asset Administrators (IAA) have delegated responsibility for the operational use of information assets and/or record sets.

4.8 **Heads of Service**

The responsibility for local records management (including retention and disposal of records) is devolved to the Heads of Service. Heads of Service within the CCG have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the CCG's records management policies. Heads of Service are responsible for ensuring that they and their staff are familiar with this policy and its associated procedures. They must ensure that any breaches of the policy are reported, investigated and acted upon.

4.9 **All Staff and Governing Body Members**

Records management compliance is an obligation for all staff and governing body members. Staff and governing body members should note that there is a Non-Disclosure of Confidentiality Information clause in their contract and that they are expected to participate in induction training, annual Data Security Awareness training and awareness raising sessions carried out to inform and update staff on records management issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which will be investigated and managed in line with the CCGs disciplinary policy and must be reported to the IG Lead/DPO and (in the case of health or social care records) the Caldicott Guardian.

All staff and governing body members are personally responsible for compliance with our policies and procedures in relation to Data Protection and Confidentiality.

5.0 Legal and Professional Obligations

5.1 All NHS records are public records under the Public Records Act 1958. This provides statutory obligations upon the CCG. The organisation will take actions as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice for Health and Social Care, in particular:

- The Data Protection Act 1998 and following its repeal, the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017)
- Access to Health Records Act 1990
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- The Human Rights Act 1998
- Protection of Freedoms Act 2012
- Caldicott Principles
- NHS Digital Guide to Confidentiality in Health and Social Care 2013
- The Common Law Duty of Confidentiality
- Health and Social Care (Quality and Safety) Act 2015
- The Nursing and Midwifery Council Code of Professional Conduct

and any other new or existing legislation affecting records management.

6.0 Records Management Procedures

6.1 Records are held to ensure that information is available within the CCG:

- To support the care process and continuity of care.
- To support day to day business of a CCG.
- To support evidence based practice.
- To support sound administrative and managerial decision making.
- To meet legal requirements, including requests from patients under the General Data Protection Regulation (EU) 2016/679, Data Protection Act and Access to Health Records Act 1990.
- To assist clinical and other audits.
- To support improvements in clinical effectiveness through commissioning/research and also to support archival functions by taking account of the historical importance of material and the needs of future research.
- Whenever and wherever there is a justified need for information, and in whatever media it is required.

6.2 In order to ensure records can be identified and retrieved when needed all staff should follow the guidance provided;

- Corporate Records Management Guidance (**Appendix A**)
- Guidance on Creating a Corporate Filing Structure (**Appendix B**)
- Patient Record Keeping Best Practice (**Appendix C**)
- Good Practice Data and Information Quality Standards (**Appendix I**)

6.3 Records must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails should track all use and changes. Records must be held in a robust format, which remains readable for as long as records are required.

All individuals undertaking roles and responsibilities on behalf of the CCG are responsible for the safe custody of records in their use. Personal confidential information must be handled in accordance with data protection legislation, the Records Management Code of Practice for Health and Social Care and any other guidance.

6.4 To ensure quality and continuity of operational services all records should be accurate and up to date. Records and record keeping should be kept according to professional guidelines. Local procedures should be developed to ensure data quality for both manual and electronic records. These procedures should be passed on to all staff and governing body members who are responsible for recording the information. It is also essential that these procedures are reviewed and updated regularly.

6.5 Staff with clinical record handling responsibilities should follow the appropriate legal and professional guidance at all times.

7.0 Tracking of Records

7.1 Accurate recording and knowledge of the whereabouts of all records is crucial if the information they contain is to be located quickly and efficiently.

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

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

7.3 Further guidance on tracking clinical records is provided in **Appendix D.**

8.0 Manual Record Storage

8.1 Storing Current Paper Records

When a record is in constant or regular use, or is likely to be needed quickly, it makes sense to keep it within the area responsible for the related work. Storage equipment for current records will usually be adjacent to users i.e. their desk drawers or nearby cabinets, to enable information to be appropriately filed so that it can be retrieved when it is next required. Records must always be kept securely and when a room containing records is left unattended, it should be locked. A sensible balance should be achieved between the needs for security and accessibility.

There is a wide range of suitable office filing equipment available. The following factors should be taken into account:

- Compliance with Health and Safety regulations (must be the top priority)
- Security (especially for confidential material)
- The user's needs
- Type(s) of records to be stored
- Their size and quantities
- Usage and frequency of retrievals
- Suitability, space efficiency and price.

8.2 Digital and other media records

- Follow guidance within **Appendices A, B and C** and instructions from The Health Informatics Service.

9.0 Records in Transit

9.1 Labelling and Packing

If records are being delivered to another location they should be enclosed in envelopes or opaque wallets and sealed for transfer. Any records that may be damaged in transit should be enclosed in suitable padding or containers.

For larger quantities, records should be boxed in suitable boxes or containers for their protection.

Each box or envelope should be addressed clearly and marked confidential with the sender's name and address on the reverse of the envelope and signed for on receipt. In the case of communications relating to healthcare and other sensitive issues it may be more appropriate not to include information on the outside of the envelope other than a Box No if available.

There are various options if records are to be mailed, such as recorded delivery, registered mail etc. When choosing options staff should consider the following: -

- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
- Does the mail provider offer "track and trace" options and is a signature required on delivery?

In addition, the number of records per envelope should be considered. It is recommended that no more than 20 records should be placed in one envelope. Ensure the correspondence is suitably secure. Seek guidance from the IG Team in relation to secure transfer of responses. Transit envelopes must <u>not</u> be used for sending records.

Items sent in any internal mail system should be fully addressed, sealed and marked private and confidential if appropriate.

For further advice please contact the Information Governance Team.

9.2 Handling and Transporting Records

- No-one should eat, drink or smoke near records.
- Clinical records being carried on-site e.g. from the archive storage to the department, should be enclosed in an envelope.
- Records should be handled carefully when being loaded, transported or unloaded. Records should **never** be thrown.
- Vehicles must be fully covered so that records are protected from exposure to weather, excessive light and other risks such as theft.
- No other materials that could cause risks to records (such as chemicals) should be transported with records.
- Vehicles containing records should be locked in the boot so that they are kept out of sight, particularly when the vehicle is stationary.
- Records should only ever be taken off site with the approval of the line manager. Security of these records should be paramount, especially in the case of confidential records. The local records manager and/or the Information Governance Team can provide advice on the precautions to take. Individuals are responsible for the safe custody of records in their use both on and off CCG or client premises. Personal confidential information must be handled in accordance with Data Protection legislation.
- Records should not be left unattended and visible. If the record is to be taken home, it must be stored securely. It is essential that any such records are tracked out of the organisation so that staff are aware of the location of the record.
- Within the CCG, faxed information should be transferred internally through the use of 'Safe Haven' fax machines ensuring the maintenance of confidentiality. For further guidance refer to the Safe Haven Guidelines and Procedure within the Confidentiality and Data Protection Policy.

10.0 Incident Reporting

If a record is missing, lost or inappropriately disclosed it should be reported to the relevant line manager as soon as possible and the incident should be recorded on the CCG incident reporting system.

Incidents involving the loss of any records containing personal data should be reported promptly and the IG Lead, DPO and SIRO should be informed (in the

case of patient data related incidents, the Caldicott Guardian should also be informed). Certain losses may need reporting externally to the Information Commissioner. The DPO will be responsible for ensuring that the Integrated Governance Committee are aware of any breaches of this policy and for overseeing any investigations or action plans.

11.0 Retention of Records, Archiving and Disposal

11.1 It is a fundamental requirement that all CCG and client 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.

11.2 The CCG has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care. See the CCG Records Retention Schedule on Skyline:
http://skyline.wakefieldccg.nhs.uk/Interact/Pages/Content/Document.aspx?id=1873&SearchId=

If a particular record is not listed within the schedule, advice must be sought from the Information Governance Team who will establish the retention period in consultation with the local records manager, relevant IAO and the Information Governance Alliance.

11.3 The CCG will ensure compliance with any local or national judicial instruction to retain (past the designated retention time) certain categories of record which may fall under the scope of an inquiry or inquest.

11.4 The length of the retention period depends upon the type of record and its importance to the business of the CCG and its clients. The destruction of records is an irreversible act, whilst the cost of keeping them can be high and continuing.

11.5 Data Protection legislation (Article 5 (e) of the GDPR) does not permit the keeping of personal information for longer than is necessary for the purposes for which it is being processed. There are some circumstances where personal data may be stored for longer periods (e.g. archiving purposes in the public interest, scientific or historical research purposes).

Recital 39 of the GDPR states that the period for which the personal data is stored should be limited to a strict minimum. In relation to personal data the CCG follows the record retention approach set out in 11.2.

11.6 It is particularly important under both Data Protection and Freedom of Information legislation that the disposal of records – which is defined as the point in their lifecycle when they are either transferred to an archive or destroyed – is undertaken in accordance with this policy.

11.7 Any documents identified as requiring permanent preservation must be transferred to the appropriate repository e.g. National Archives Approved

Places of Deposit. Disposal decisions made following an appraisal must be recorded. http://www.nationalarchives.gov.uk/archives-sector/our-archives-sector-role/legislation/approved-places-of-deposit/

11.8 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. The storage of closed records should follow National Archives guidance relating to environment, security and physical organisation of the files.

11.9 The destruction of records is an irreversible act. Many NHS records contain sensitive and/or confidential information and their destruction must be undertaken in secure locations and proof of secure destruction may be required. Destruction of all records, regardless of the media, should be authorised and should be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure. A record of destruction must be kept. See **Appendix E** and **Appendix F**.

11.10 When destroying records the following must be undertaken:

- The intended destruction must be authorised. See the approval form at **Appendix F**.
- 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 by the Information Governance Team.
- 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.

11.11 Further guidance on archiving and disposal of records is attached in **Appendix A**.

12.0 Scanning

12.1 For reasons of business efficiency or in order to address problems with storage space, the CCG may consider the option of scanning paper records into electronic records.

12.2 Where this is proposed, the scanning equipment must be of a quality to meet the British Standards and in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008) and the scanning guideline should be followed – see **Appendix E**.

13.0 Data and Information Quality

13.1 Data quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever this is required. Data quality is vital to effective decision making at all levels of the organisation.

13.2 It is also important to ensure that the data quality of personal data is of a high standard in order to comply with the Data Protection Principles enshrined within data protection legislation i.e. 'accurate and, where necessary, kept up-to-date' and to satisfy the data quality requirements within the NHS Care Record Guarantee.

13.3 The standards for good data quality are reflected in the criteria below. Data needs to be:

- Complete (in terms of having been captured in full).
- Accurate (the proximity of the data to the exact or true values).
- Relevant (the degree to which the data meets current and potential user's needs).
- Accessible (data must be retrievable in order to be used and in order to assess its quality).
- Timely (recorded and available as soon after the event as possible).
- Valid (within an agreed format which conforms to recognised national and local standards).
- Defined (understood by all staff who need to know and reflected in procedural documents).
- Appropriately sought (in terms of being collected or checked with the service user during a period of care).
- Appropriately recorded and free from duplication.

Please refer to the guidance document **Appendix I**.

13.4 Within any record keeping system, there is a primary instance which can be considered the version that needs to be kept and this will normally be held by the person or the team with the function to provide the service or activity about which the records relates.

It is not necessary to keep duplicate instances of the same record unless it is used in another process and is then a part of a new record. An example of this is incident forms. Once the information is transcribed into the incident management system, there is no longer a need to hold the (now) duplicate instance of the original form used to record the incident.

13.5 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.

13.6 For guidance on data quality management please refer to the guidance document in Appendix I

14.0 Using NHS Numbers

14.1 The NHS number is a unique way of identifying patients in NHS systems. With this in mind it is imperative that this is recorded correctly and in all systems where patient information is present.

14.2 The Personal Demographics Service (PDS) and Exeter will be used to obtain verified NHS numbers i.e. NHS number status and as PDS has significant historic data it will enable record matching process and support the resolution of data anomalies.

15.0 Using Electronic Signatures

15.1 In order to ensure the security and legal validity of an e-signature the use of a scanned representation of a handwritten signature must be recorded by the corporate team.

15.2 Images of signatures should be used only where a clear audit trail of authorisation including written permission has been granted by the signatory. Though it is only a small deterrent to copying images of signatures, they should be sent outside the organisation in PDF files rather than emails, Word documents or spreadsheets. The PDF files should be created with the highest levels of protection.

15.3 Documents containing the image of another person's signature must not be sent without a clear audit trail of authorisation including written permission of the person concerned, unless prior delegation and clearance procedures have been agreed. In such cases:

- such agreement, including the list of recipients, must be obtained in advance for each document.
- the content of the document must not be changed after authorisation to issue it has been obtained
- once such a document has been sent, it must not be sent again (or to additional recipients) without further explicit authorisation.

15.4 All staff who allow a proxy to access their email account or scanned signature must ensure that the proxy is informed of the limits of their authority in the sending of emails or signing documents on behalf of the member of staff.

15.5 Electronic signatures should not be used in transactions where there is a legal requirement for a written signature, for example in the signing of a deed or other document where the signature is required to be witnessed.

16.0 Emails as Records

16.1 All emails sent or received by anyone with a CCG email account can be classed as a CCG record.

16.2 If an email does relate to the conduct of the CCG's business such as information likely to be required for the determination of actions or decision making then it is considered a record.

16.3 All emails could be produced in a Court of Law, under the eDiscovery regulations.

16.4 To manage email messages appropriately, members of staff need to identify email messages that are records of their business activities and decision making. It is important that email messages and their attachments which are considered as 'records' are moved from individual mailboxes and managed in the same way as other records.

16.5 Emails have differing retention periods dependant on their subject and content. Emails are subject to the same records management principles as the equivalent record in any other format. Please refer to the CCG Records Retention Schedule for details of the minimum retention period for specific record types.

16.6 Email should only be used to send confidential information where it is sent between approved secure email addresses (e.g. NHS Mail, COIN sender and receiver with password protected attachment) or where it is adequately protected through the use of an encryption solution e.g. using THIS Encrypt solution, WinZip version 9.0 or above or Sophos encrypt. Seek advice from the Information Governance Team if you require advice on emailing information securely.

16.7 The Email system should not be used for long term storage. Emails considered as records should be stored in the relevant filing system and then be deleted from the inbox/sent items box. See **Appendix H** for instruction on how to save email to a network drive location.

16.8 Emails sent from or to personal email accounts which relate to work matters will be considered public records for the purpose of legislation such as the Freedom of Information Act 2000.

17.0 Digital, Audio, Visual, Photographic, Text and other Electronic Records

17.1 All records are subject to this policy regardless of the format in which they are held.

18.0 Access to Records

18.1 Under the new data protection legislation data subjects have the right to access personal information held about them by the CCG, subject to certain exemptions. Please refer to the Subject Access Request and Access to Health Records Procedure (**Appendix J**).

18.2 Under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 individuals have the right to access corporate information,

subject to certain exemptions. Please refer to the Freedom of Information and Environmental Information Regulations Policy.

19.0 Decommissioning of Buildings/ Vacating Premises

19.1 It is the responsibility of the CCG management team to undertake a visual check of CCG premises that are being closed to ensure that all assets of the CCG (including information assets) have been removed.

20.0 Records Management Systems Audit

20.1 The CCG, supported by the Information Governance Team will audit its records management practices for compliance with this framework. The CCG has the ability to use Internal Audit to seek an opinion on the overall adequacy and effectiveness of the CCG's systems and this will be determined as part of the local Internal Audit Plan.

20.2 The audit will:

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

20.3 The results of audits will be reported to the CCG's Audit Committee.

20.4 Audits of individual corporate record systems will be conducted in line with **Appendix A**.

20.5 Clinical Record Audits will be conducted as appropriate in line with good practice and professional guidelines.

21.0 Information Asset Registers

21.1 All information assets (record collections) held by the CCG must be included in an Asset Register which should include as a minimum:

- Name of Information Asset
- System Type
- Description of the purpose of the asset
- Purpose of processing
- Data Held
- Any Joint Data Controllership
- Physical location of the asset
- Class – e.g. personal or business

- Components and format e.g. database, paper files
- Name of Information Asset Owner
- Any special categories of personal data and description of that data
- Lawful basis of processing of personal data
- Critical assets
- Risk Assessment
- Business continuity plans
- Access controls
- Retention time of the information asset
- Description of manner of secure destruction of the information asset
- Additional information e.g. data flows

22.0 Clear Desk Policy

22.1 Under no circumstances should personal confidential information be left out in the open e.g. on an unattended desk or on a computer screen or any place visible to the public. Where rooms containing records are left unattended, they must be locked. Personal confidential information should be stored securely in either a locked cabinet or within a secure environment on a computerised system.

22.2 When storing electronic records, care must be taken to ensure that no personal identifiable information e.g. health records, human resources records, are stored in shared folders or on the local drive of the PC. All records of this nature must be stored within a folder that can only be accessed via a password or within a specific secure area. Restricted access can be set up by contacting The Health Informatics Service Desk.

22.3 All staff should be aware that non-personal corporate information may be confidential and similar care should be taken of these records.

23.0 Training

23.1 Records Management will be a part of induction training and is mandatory for all staff. The CCG will identify the information governance training needs of key staff groups taking into account role, responsibility and accountability levels and will review this regularly through the PDR processes in relation to those staff with a particular responsibility for records management.

23.2 It is the line managers' responsibility to ensure that all staff are made aware of their record keeping responsibilities through generic and specific staff training and guidance so that they understand:

- what they are recording and how it should be recorded;
- why they are recording it;
- how to validate information with the patient or carers or against other records – to ensure that staff are recording the correct data;
- how to identify and correct errors – so that staff know how to correct errors and how to report errors if they find them;

- the use of information – so staff understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and
- how to update information and add in information from other sources.

23.3 All CCG staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance. Line managers must ensure that all new employees are provided with the IG User Handbook and an explanation as to the service's records management arrangements including the controls applied to paper and electronic files containing person identifiable and business sensitive information.

24.0 Implementation and Dissemination

24.1 Following approval by the Audit Committee this policy will be disseminated to staff via the CCG's intranet and communication through in-house staff briefings.

24.2 This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

25.0 Monitoring Compliance and Effectiveness of the Policy

To be assured that this policy is being implemented, key elements will be monitored for compliance.

- **Successful completion of the annual information governance work plan** Records management work packages will be monitored for successful completion by the Audit Committee.

- **Satisfactory achievement of the requirements of the Data Security and Protection Toolkit.** The Audit Committee will monitor overall progress through receipt of quarterly reports and take action to address any concerns and deficiencies will be noted and reviewed at subsequent meetings.

- **All staff receive annual training and competency test in Data Security Awareness (which includes record keeping good practice).** The Audit Committee will monitor progress via the Workforce Report.

- **Incidents are reported and all serious information governance issues are reported by the SIRO at Governing Body level and in Annual Reports.**

26.0 Associated Policies and Procedures

This policy should be read in conjunction with:

- CCG Records Retention Schedule
- Confidentiality and Data Protection Policy and Procedures
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Governance Policy and Framework
- Information Security Policy (incorporating Network Security)
- E-Communications and Social Media Policy and Procedure
- Integrated Risk Management Framework
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy and Procedure
- Anti-Fraud, Corruption and Bribery Policy
- Whistleblowing Policy

And their associated procedures (including but not limited to):

- Subject Access Request and Access to Health Records Procedure
- Interagency Information Sharing Protocol
- Data Protection Impact Assessment and Information Governance Checklist
- Safe Haven Guidelines and Procedure
- Confidentiality Audit Procedures

Appendix A

Corporate Records Management Guidance

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 to their lifecycle to their eventual disposal. It is the aims of the organisation to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

Corporate Records can be considered records which contain the following:

- all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints);

Good records management will also help to Information Asset Owners with the Information Asset audit and the information flow mapping exercise.

Corporate Records

Records management is crucial to all NHS organisations, especially during a time of transition. If records are not managed effectively, the organisation would not be able to function as required and expected, and to account for what has happened in the past or to make decisions about the future. Records are a fundamental corporate aspect and are required to provide evidence of actions and decisions, enable the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the General Data Protection Regulation (EU) 2016/679 and Data Protection Act and the Freedom of Information Act 2000.

Corporate records also support strategic decision making and enable the organisation to protect the interests of staff, patients, public and other stakeholders.

Corporate Records should:

- be accurate and complete
- be arranged systematically
- should be sufficient to enable other members of staff to carry out their tasks
- should demonstrate compliance with legal and regulatory requirements.

Paper Records

- A uniform filing system should be implemented to ensure that documents are grouped appropriately and consistently. Records that are frequently used should be stored within secure filing cabinets or secure areas (locked rooms, coded areas). Records that are not frequently or not used at all should be stored in secure rooms or in Iron Mountain. If records are no longer needed and do not need to be kept according to the retention timeframes, the records should be destroyed.

- The filing system should also be kept simple and easy for all to understand. A standard operating procedure will ensure that all staff within your assigned area can follow the same filing procedure. Refer to Guidance on Creating a Corporate Filing Structure (**Appendix B**).

- Should you have many categories of information associated to the same record, cross – referencing is a key element to identify documentation which is connected to the same record.

- Agree with line management whether records are to be kept manually or electronically. This will help determine the master record.

- Restrict 'creating folder responsibility' to a limited number of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to be granted permission from the lead administrator/Information Asset Administrator.

- Paper files should be labelled accurately and helpfully. Labels should be brief, accurate, have a meaningful description of the contents, and intelligible to both current and future members of staff.

- Where appropriate templates should be used.

- Version controls should be applied and periodically reviewed.

- All paper files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived or destroyed. It would be useful to have a tracker card to include who uses the file, location of where the file is situated and also retention review date.

- Should the file contain personal identifiable or sensitive information, it is important not to add this to the title of the record and the file should be kept in a secure location. Page numbering confidential files will confirm if pages have been removed or are missing.

- Permission to access personal identifiable and sensitive information should be restricted to a limited number of staff who requires access.

- Information Asset audits should be carried out, this will prevent duplication and provide easier access to information readily for requests/enquiries.

- Records should be reviewed on a periodic basis to ensure that destruction rules apply.

Electronic Records

- Name electronic files accurately, they should be simple and easy for all to understand. A standard operating procedure will ensure that all staff within your assigned area can follow the same filing procedure.

- Restrict ‘creating or deleting folder responsibility’ to a limited number of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to granted permission from the lead/information asset administrator.

- All electronic files should be reviewed at the end of every financial year. This will identify if records need to be retained and archived.

- Each assigned area should compile a list of standard terms and uniform terminology as naming conventions for files and folders.

- Version control should be applied and periodically reviewed.

- Records with personal identifiable and sensitive information should be controlled through the use of logins, restricted folder access and encryption when appropriate.

- Once a project is completed, all associated electronic documentation should be contained in a folder, accurately named/dated and stored within a secure folder on the organisation’ network. This will decrease storage space and will keep all common documentation together.

- Desktop and portable computing devices should be located in facilities with restricted and monitored entry. If this is not possible devices should not be left unattended. Laptops and portable devices must be encrypted and stored securely out of sight and when not in use.

Record Keeping Audit

It is important that teams conduct a record keeping audit. The information collected from the audit will enable the assigned Information Asset Owner;

- To understand what records are available within the department
- Assess the staff knowledge of records management
- Identify if the organisation’s records management policy and procedures are adhered to by staff and have been implemented within your assigned area.
- Identify any gaps in record management processes
- To help collate information for the information asset register and the information mapping exercise.

Archiving, Retention and Disposal Process including Off-site Storage

To avoid breaches, incidents and information loss, it is important for departments to ensure that retention, retrieval and disposal procedures are followed. Department Managers should coordinate this function within your assigned area. Members of staff may also ask you to coordinate the archiving and disposal of records.

The current contract for offsite archive storage sits with Restore plc.

Offsite Storage Archiving Process

CCG employees must consult the CCG IG Lead/ Corporate Lead regarding archiving requirements.

Any records sent to offsite storage remain the responsibility of each team.

Senior Managers / Information Asset Owners have the responsibility to ensure effective and relevant file management systems are in place for information held within their teams.

Following this process will avoid teams duplicating or, mismanaging information therefore ensuring information security.

Onsite archiving

Each team should have a programme of archiving for records held onsite. The following should be used when records have been approved for destruction:

1. **Confidential Shredding** Teams should ensure all confidential documents are disposed of confidentially. Confidential waste bins are available on site. Confidential waste must not be disposed of within recycling and personal waste bins. Black bin liners should not be used to store or dispose of confidential information.

2. **Destruction of Electronic Equipment** All electronic equipment that store personal and sensitive information i.e. CDs, DVD–Roms, USB sticks, computers etc. require specialist destruction. It is important to follow the IT provider's secure destruction process. Should you have any queries or would like to request destruction of electronic equipment, please contact the Health Informatics Service Desk.

What to do in the Event of Missing Health and Corporate Records

Missing records pose a serious risk to the organisation and it is therefore vital that a tracing procedure is undertaken should a record be misplaced. The following steps should be taken:

1. Highlight that a record is 'missing' to the assigned Information Asset Owner (IAO) and work colleagues as soon as this becomes apparent.

2. Undertake a thorough search for the record in the places you would normally expect to find it. Search in the place you would normally expect to see the record but look either side, above and below where it should be filed. If the record is held electronically search in other folders or conduct a ‘search’ within your files.

3. Should the record remain missing after your search, you will need to contact the Information Governance Team, complete an Incident form and make an assessment of the risk to the organisation should the record not be found.

4. Keep a list of all the places that have been searched.

5. The Senior Information Risk Owner (SIRO)/Caldicott Guardian/IG Lead should be informed of the loss by the relevant IAO or Information Governance Team.

The Information Asset Owner (IAO) and Information Governance team should be informed if the record is found.

Appendix B

Guidance on Creating a Corporate Filing Structure

Records are not accessible when they are on the local disk of your PC/device/workstation or on your own personal drive on the network; no one other than the originator can find them. They must be stored in a shared folder area on the central file server in a location defined by the Head of Service/Information Asset Owner.

As a result clearly defined structures for departmental shared folders are essential to enable staff to access files in a quick and effective manner. Defining an outline file structure with the involvement of the whole team will mean that users will have a clearer understanding of where to store and retrieve documents from.

When handling any type of record, it is important to make the distinction between a record and a document. In the context of this guidance, a document becomes a record when it has been finalised and become part of the CCG corporate information. With paper records, a further distinction must be made between the original record and a copy of that record. The original record should only be held in the corporate record-keeping system, and not in staff desk drawers, etc.

The following applies to both electronic and manual records:

Creation of Information

When a corporate record is created the name of the document, version number and date should be detailed in the footer.

Every document/record created should have a predetermined 'shelf life', a date when it should be reviewed, disposed of, archived or destroyed/deleted. Information as it is gathered should fall into a specified classification as exampled.

Classification of Information

Define classification:

- ***Public***
- ***Internal***
- ***Confidential***
- ***Management in Confidence***

All information should be stored in a manner appropriate to its classification, as follows.

- **Public**

  Anyone: Information that is freely available to anyone and does not require any safe storage.

- **Internal**

  Organisations: Information available to anyone within the Organisation, the information is not marked in any way and does not require any safe storage. However, if taken away from the organisation's premises i.e. employees who work from home, should not leave this information unsecured in their home or in public places.

- **Confidential**

  Sensitive: Information must be **safe.** Accessed only by those who have right to know. Information on computers must be safeguarded by the use of passwords and access rights. Paper files must be stored in lockable cabinets or similar at the end of each day or when not being used. This applies regardless of the format which this information is held on e.g. paper, disk, files, tapes, faxes, post.

- **Management in Confidence**

  Restricted: Information restricted to certain individuals, care should be taken that this information is not read or heard by people in the organisation that do not need to know it. Therefore similar controls to the **'confidential'** must be implemented e.g. password protection of documents, locking away information etc. Documents should be labelled as 'Management in Confidence'.

Classification often indicates how the information can be used or shared and its specified required retention period, review date or disposal. Access to these files is governed by the user's personal access rights.

It is important that all information/records are stored in line with:

- Health & Safety Regulations
- Confidentiality and Data Protection Policy and Procedures
- Records Management Code of Practice for Health and Social Care

Categories of Information

Define Category:

- **Business**
- **Operational**
- **General**
- **Other**

Each category will have pre agreed sub folders to define and store/file the information in the most appropriate place. Awareness training and clear guidance will encourage a consistent approach to document management.

Example sub folders:

Business/Governance
Statutory Requirements:
Board Meetings
Public Meetings
Financial
Annual Reports
Board Agenda
Board Minutes

Operational
DoH Reporting
Health Records
Analytical Reporting
Minutes & Agendas
Purchase & procurement
Policy & Procedure
Projects open/closed
Estates/ Engineering
IM&T
Personnel/ HR

General
Administration
Correspondence
Complaints
General Minutes & Agenda
Public Awareness
Staff Awareness
Training
Projects
Email
Faxes
Personal

Once the appropriate category has been selected, the electronic storage requirement should be defined at the same time as building a concise set of sub folders. The IAO should ensure appropriate access controls to the folder area are in place, so that only those with a business requirement to access the information are able to do so. This will reduce the risk of misfiling and give confidence to many users, providing a better use of staff time. Restricting access to shared folders can be requested through the Service Desk (please refer to **Appendix G** of Records Management and Information Lifecycle Policy and Procedures).

Name files so that they can easily be found at a later date. **It is not good practice to name a file with a person's name**.

Appendix C

Patient Record Keeping Best Practice

Introduction

The accuracy, legibility and timeliness of entries in patient records are essential to good records management.

The quality of the patient notes and the condition of the patient record is therefore paramount. To assist this, patient records will be:

- bound securely in agreed NHS record patient files.
- kept securely within the environment/teams in which they are created to protect them from damage and environmental conditions.

DO…

Be factual, consistent and accurate.

- Check the patient's contact and address details routinely for any changes and update the master record. Inaccurate contact and address details may result in important letters being mislaid, or the incorrect identification of individuals.
- Write records as soon as possible after an event has occurred, providing current information on the care and condition of the patient.
- Write clearly, legibly and in such a manner that they cannot be erased.
- Write in such a manner that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read clearly.
- Accurately date, time and sign, with the name of the author being printed alongside the first entry.
- Write in chronological order, so that the pattern of activities can be followed through the series of entries.
- Write in **BLACK INK**, for reproduction purposes, must be in permanent black ink to prevent alterations and aid copying, except in specific circumstances as outlined below.
- Ensure records are readable on any photocopies.
- Check and use the NHS Number where possible.
- Ensure records are clear, unambiguous, concise (where possible) and written in terms that the patient can understand. Abbreviations, if used, should follow common conventions and should be in full when first used with abbreviation in brackets afterwards.
- Ensure that records are consecutive and chronological.
- Use standard coding techniques and protocols (for electronic records).
- Ensure that any space left at the end of a line must have a line run through it. This is to prevent anyone adding a retrospective entry, thus altering the meaning of the entry.

Be relevant and useful

- Identify problems that have arisen and the action taken to rectify them.
- Provide evidence of the action planned, the decisions made, the information shared and outcomes of actions taken.
- Provide evidence of actions agreed (including any consent to share).
- Ensure that if there is a requirement to document opinions and ideas that it is clearly stated that they are such. All opinions and ideas must however be based on fact and the rationale for the professional opinion must be clearly stated.

And include

- Observations: examinations, tests, diagnoses, prognoses, prescriptions, other treatments if applicable.
- Relevant disclosures– pertinent to understanding cause or effecting cure/treatment.
- Facts presented.
- Correspondence.

DO NOT

- Use unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements.
- Use correction fluid to amend an error in the written entry. It must be crossed through with a single line and initialled by the person crossing out the entry, and the corrected entry written next to it, or the sentence continued. The original entry must be readable.
- Squeeze words onto a line, as this could make the entry unclear and ambiguous.

Remove sheets of paper or other items from a patient file without proper agreement. If a file is becoming too thick with paper, then the solution is to start another volume.

Appendix D

Keeping patient, client or personnel information physically and electronically secure

For all types of records, staff working in offices where records are in use must:

- Shut / lock office doors
- Lock cabinets containing records when not in use and when unattended.
- Wear building passes / ID if issued.
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- Not tell unauthorised personnel how the security system operates.
- Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after completion of treatment.
- Stored securely within the office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorized persons.
- Held in secure storage with clear labelling indicating sensitivity (though not reason for sensitivity) and permitted access.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have a need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords, or using names or words that are known to be associated with them.
- Always clear the screen of a previous patient / client / staff record before seeing another.
- Use a screensaver (preferably with password) to prevent casual viewing of confidential information by others.
- Never share a smart card or leave their smart card unattended in a computer

Appendix E

Scanning Records and Destruction of Paper Records

When paper records are scanned the quality and integrity of the scanning process and resultant scanned image must be verified.

General

- When scanning paper documents into electronic records, you should do so in a way that preserves content, ensures business continuity of workflow, and is secure and reliable.
- Documented protocols should be in place for the summarising, filing, scanning and destruction of all such documents.
- Ensure that original records are not disposed of until the quality of the scan has been verified.
- When using third party scanning services ensure that there is a contract in place with the third party detailing specific information governance and data quality responsibilities.
- When transferring documents or allowing access to 3rd party scanning services, ensure that appropriate physical security controls are in place.

The Information Asset Owner should consider whether records should be subject to particular controls so as to ensure their evidential value in line with the Code of Practice 'BIP 0008-1:2008: Evidential weight and legal admissibility of information stored electronically and be able to demonstrate, if required, by showing them to:

a) Be authentic, that is, they are what they say they are;
b) Be reliable, that is, they can be trusted as a full and accurate record;
c) Have integrity, that is, they have not been altered since they were created or filed;
d) Be usable, that is, they can be retrieved, read and used.

Scanning

There are two ways a document can be scanned;

- Stored as an image file (usually a PDF)
- The computer reads the image and turns it into a word-processed document, known as an optical character recognition (OCR)

It is strongly recommended that all scanned documents are stored as PDF images.

Resolution of 150 x 150 dpi, is suitable for document archiving.

OCR is only acceptable if the original image is stored as well.

All documents to be scanned should be thoroughly checked for the following prior to scanning and a note made of the quality issues found:

- Missing text at edges of page

- Skewed or off-centre, rotated or backward pages
- Missing page numbers
- Materials (sticky notes, paperclips, dust, rubber bands etc.) included on the paper record
- Presence of digital artefacts (such as regular, straight lines across page)
- Issues with legibility of text (contrast, pixilation etc.) - Feint and blurred originals will only ever reproduce as feint and blurred text.

The IAO should undertake a risk assessment of whether all scanned documents should be quality checked or whether a process of regular and systematic spot checks will be sufficient to ensure scanned document quality. Quality checks should ensure:

- All pages have scanned successfully
- All pages are in the correct sequence order
- No missing text at edges of the scanned image
- Scanned pages are not skewed or off-centre,
- Rotated or backward.
- No missing page numbers
- Clean edges, clear contrast, and legible text (text density, character size, line widths, and letter clarity).
- No unwanted materials (sticky notes, paperclips, dust, rubber bands etc.) included in the scanned image.
- No presence of digital artefacts (such as regular, straight lines across scanned image).
- No pixilation is not too light or too dark and has no loss of detail in highlight or shadows.

The final scanned documents become the primary record of events and could be used in court as evidence.

Destruction

Once a document has been scanned, stored in an appropriate format and quality checked, the paper document may be destroyed in line with the Approval to Permanently Destroy Information in **Appendix F**.

All documents to be destroyed must be securely destroyed by shredding or placing in a confidential ‘shred’ bin.

Appendix F

Certificate of Records / Information Permanent Destruction

This form (Certificate of Destruction) must be completed in relation to any records that have been stored / used within NHS Wakefield CCG and have been approved for permanent destruction**.**

Please note that permanent destruction MUST include any existing secondary copies of electronic records held by the CCG.

Method of Destruction Used

Please indicate, for each item identified, the method of destruction used. Please note that if a 3rd Party supplier has been used, a copy of their certificates must be attached to this form.

RECORD DISPOSAL NOTIFICATION (Number _____)

The following record/s has been disposed of:-

Paper Copy ☐

Electronic ☐

Photographic ☐

Audio (e.g. tapes) ☐

Visual (e.g. videos) ☐

Other ☐

Please specify ……

Subject: - ……

Type: - ……

Period Range: - ……

Retention Period Applicable: - ……

Status: - Confidential ☐

Open ☐

Disposed of by: - Shredding/Confidential Waste ☐

Normal Waste ☐

Approval to Permanently Destroy Records / Information

By signing this document, you are confirming the following

- Records identified for destruction have reached or exceeded the minimum retention period as set out in the CCG Records Retention Schedule and have been reviewed for any business requirement to continue to retain them.
- Records identified for destruction do not fall under the scope of any Inquiry e.g. Independent Inquiry into Child Sexual Abuse or any legal proceedings.
- The records have been verified to include all copies, including any local copies such as those duplicated for Business Continuity / Disaster Recovery plans.

Member of staff requesting the destruction:

Signed: ……

Print Name: ……

Position Held: ……

Department: ……

Date: ……

Authorisation from Information Governance Lead

Signed: ……

Print Name: ……

Position Held: ……

Department: ……

Date: ……

Fully completed and signed forms must be passed to the Information Governance Team and retained indefinitely as proof of destruction

Appendix G

Guidance on restricting network/folder access

Restricting network access to folders is the most efficient and effective way to protect the confidentiality of records. It also means that you are not reliant upon multiple passwords that can be easily lost.

All teams require as a necessity a centralised storage area and as a consequence all teams have been set up with a single team folder on the network. Therefore, restricting access to your team folder, whereby only nominated individuals can access your folder, should be a straightforward process that The Health Informatics Service (THIS) will provide.

Different Types of Network Access

There are different types of access rights you can apply:

Full Access
Named individuals gain full read and write access to the folder. They can view and edit all records and can save any file to the folder.

Read-Only Access
Named individuals can access the folder but can only view documents. They cannot edit records and they cannot save any file to the folder.

Browsing Access
Named individuals have full access to the folder. Everyone else who has access to the network drive can view the contents of the folders but cannot view any records.

Setting network access for staff should form part of the new starter process. Help reduce the need for applying passwords to documents by setting appropriate access controls instead – passwords are easily forgotten or lost and it is much easier for the Service Desk to change access rights than unlock a password protected document.

Who Should Have Access to the Team Folder

Ultimately it is the Information Asset Owner/Head of Service or team lead that will decide who should have access to the team folder. The normal protocol is to include all team members as well as the Head of Service. However, the manager or lead needs to use their judgement, for example, they work closely with a member of another team who would benefit from having access to the folder.

Restricting Access Within the Team Folder

It is not just at the team folder level that you can place access restrictions; you can also do this on sub-folders within the team folder where there is a need to protect confidentiality from team members. For example, most teams have a Workforce/HR.

These are normally restricted to the team manager or lead and a secretary or administrative support to complete leave requests or sickness returns.

The process for placing ‘internal’ restrictions on sub-folders is exactly the same as for placing restrictions on team folders, it is merely the details that are different.

Managing and Tracking Access Restrictions

Access rights and restrictions to your folders should be explicitly and actively managed. The current access rights to your team folder and all sub-folders have been recorded.

Naturally over time, people are removed from having access rights and new people are added in. The Information Asset Administrators must maintain this information when any changes are made to access rights on any of the folders.

When a team member leaves to work with another team in the organisation, their access rights should be removed. If the person leaves the organisation, then the person should be removed from the system entirely.

Testing Your Access Restrictions

Once the Service Desk have implemented your request to grant or amend access rights, you must test the folders with a responsible third party who should not have access. This provides assurance that the folder or folders have been set up with the correct access permissions.

You must test folder access every time a change is made to the access rights; and if no changes are made then you must do this on an ongoing basis, at least once every three months.

Testing access is a five-minute job and can be performed over the phone with the trusted third party with the third party reporting what they do and do not have access to. Any errors in access permissions that are identified must be reported to the Service Desk and rectified.

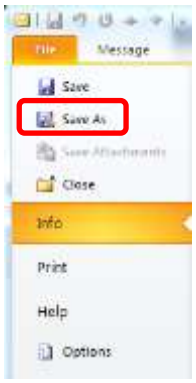
Appendix H

Saving email to a Network Drive Location

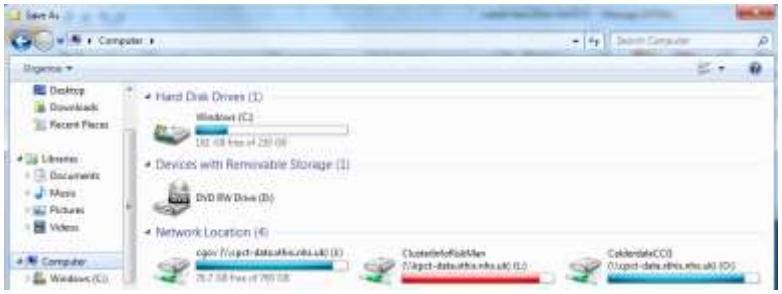
1. **Open the email you wish to save**
   Double click on the email to open it.

2. **Click on the file Tab**
   This is located in the top left of the open email (circled in red in the above image).

3. **Click on 'Save As' option.**



4. **Select the destination where you would like to save the email.**
   By double clicking on the network drive and selecting the desired Folder.



5. Save the file once the location has been selected and file name chosen

You can change the file name of the email to one of your choosing and once you are happy, simply press ‘save’.

Appendix I

Good Practice Data and Information Quality Standards

Definitions

- **Data**: Data is a collection of facts from which information is constructed via processing or interpretation.

- **Information:** Information is the result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

- **Data Quality**: Data quality is a measure of the degree of usefulness of data for a specific purpose.

These standards relate to patient/service user and staff identifiable information but the principles included are applicable to any other data/information staff may process i.e. letters, recording of minutes, etc.

There are many aspects of good quality data, the key indicators commonly are:

- **Completeness** – All mandatory data items within a dataset should be completed.

- **Consistency** – Correct procedures are essential to ensure complete data capture.

- **Coverage** – this reflects all information that is 'owned' by the CCG, including paper and electronic records.

- **Accuracy** – data must be trusted reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- **Accessible** - to those who need it. Data must be retrievable in order to be used and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist

- **Relevance** – Information should be contextually appropriate and not excessive.

- **Timeliness** - recording data must be performed in a timely manner and as close to the event as possible.

- **Validity** – All data items held on the CCGs computer systems must be valid.

    - Where codes are used, these will comply with national standards. Wherever possible, computer systems should be programmed to only accept valid entries.

- Systems will include validation processes at data input to check in full or in part the acceptability of the data wherever possible.

- Cross checking data - that the details being recorded are checked with the source at every opportunity. This could be by cross checking against accredited external sources of information, for example using Patient Demographic Service (PDS)/Exeter to check NHS numbers, or by asking the service user themselves.

- Checking for duplicate or missing data, checking for deceased patients, validating lists and synchronising systems.

Validation Methods

Validation should be accomplished using approaches that are in line with the legal powers of the CCG or using services provided by the Data Services for Commissioners Regional Office (DSCRO).

Validation should be accomplished using either of the following methods:

- Bulk reporting, which involves a large single process of data analysis to identify all areas where data quality issues exist and report to the source provider or correct them.

- Regular spot checks, which involves data analysis on a random selection of records against source material if available.

- Bulk Reporting can be used as an initial data quality tool as this will quickly highlight any areas of concern, however, further investigation may be required to identify more specific issues. Spot checks should be done on an on-going regular basis to ensure the continuation of data quality.

Where data errors are identified, appropriate mitigation is required. This includes correction or annotation, where relevant, analysis of processes and ongoing monitoring.

Data recorded manually and on computer systems must be accurate. Data accuracy is the direct responsibility of the person inputting the data.

If you have any queries or concerns about the quality of your data then please speak to your line manager or contact the Information Governance Team.

Appendix J

Subject Access Request and Access to Health Records Procedure

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Finance Officer
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager & Senior IG Officer
Date Approved:	April 2018
Committee:	Integrated Governance Committee
Version:	3.1
Review Date:	April 2020

Version History

Version	Date	Author	Status	Comment
1.0	Dec 2014	IG Associate/ Governance & Board Secretary	Approved	Policy approved by Integrated Governance Committee 18 December 2014
2.0	Dec 2016	Senior IG Officer & IG Manager	Approved	Added to Skyline
2.1	Feb 2018	Information Governance Manager	Draft	Review of policy and associated procedures. Amendments to reflect changes under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017).
3.0	April 2018	Information Governance Manager	Approved	Approved by IGC April 2018
4.1	Novemb er 2019	Information Governance Manager	Draft	Minor amendment to Appendix J 'Subject Access Request and Access to Health Records Procedure' to reflect that Subject Access Requests can be made verbally as well as in writing.

Performance Indicators

% of requests completed within statutory timeframe of one calendar month

Contents **Page**

Appendix

1. Rights of Access to Personal Data

1.1 Individuals have the right, under the General Data Protection Regulation (EU) 2016/679 (Articles 12 and 15) and Data Protection Act, to request access to, or a copy of, information an organisation holds about them. This information may be held on computer, in a manual paper system, video, digital image, photograph, x-rays, email or by any other new or existing medium or media. This is called a subject access request (SAR).

1.2 Anyone making such a request is entitled to be given a description of:

- Which data (categories) are being processed
- Details of the data controller, including contact details
- Contact details of the Data Protection Officer
- Purposes of the data processing, applicable legal basis and whether there is a statutory or contractual requirement to process data
- Other organizations that data may be shared with
- Whether there is any data processing taking place outside of the EEA
- The retention period for the data categories
- Individual rights to rectification, erasure, withdraw consent/object/opt out, data portability, ability to take complaints to the ICO.

1.3 The General Data Protection Regulation (EU) 2016/679 (Articles 12 and 15) and Data Protection Act applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990.

2. Personal Data held by a Clinical Commissioning Group

2.1 Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2 NHS Wakefield Clinical Commissioning Group (CCG) is a commissioning organisation and does not hold individual medical records except with consent as part of processes such as Continuing Care, Individual Funding Requests and Complaints or where there is a specific legal basis for doing so. The organisation also holds personal data relating to staff and Governing Body members, contractors and members of the public.

3. Subject Access Requests

The responsibility for the management of the subject access request process sits with the Governance Team with assistance from relevant members of staff.

3.1 Requests for access to personal data can be made verbally or in writing. If made in writing, there is no requirement in law to use a specific form, however the CCG has provided a form (Appendix B) for applicants to use which ensures

all the relevant information is collected and recorded to assist the applicant and the CCG.

3.2 There is no obligation for a data subject to explain why they wish to access their own personal data.

3.3 Proof of identity will be required for subject access requests (Appendix B).

3.4 Requests should generally be processed free of charge. For 'manifestly unfounded or excessive' requests only, an administrative fee may be advised based on actual costs.

3.5 The subject access requirements of the Act are for the subject to receive personal data or have remote access to those systems holding their data. Where direct/remote access is not available, providing copies of the record/documents are usually preferred over this being summarised in another format.

4. Timescales

4.1 The NHS undertakes to respond to any Subject Access or Access to Health Records request within 21 calendar days. If it is anticipated that this will take longer than the 21 calendar day period, the applicant will be informed and given an explanation for the delay.

NHS best practice recommends disclosure within 21 days where a record has been added to in the last 40 days.

4.2 The timeline commences when the CCG has received ALL of the following:

- Valid request
- Valid Identification
- Payment of a fee if request deemed "manifestly unfounded or excessive"

4.3 Under the General Data Protection Regulation (EU) 2016/679 (Articles 12 and 15) and Data Protection Act the CCG must respond to requests within one month.

5. Requests under Access to Health Records Act 1990

5.1 The Common Law Duty of Confidentiality extends beyond death.

5.2 Certain individuals have limited rights of access to deceased records under the Access to Health Records Act:

- Individuals who may make an Access to Health Records request;
- Those named executor of a will or specified in letters of administration (documentation confirming this is required);
- Any person who may have a claim arising out of the patient's death.

5.3 A Next of Kin has no automatic right of access but professional codes of practice allow for a clinician to share information where concerns have been raised.

5.4 Guidance should be sought from the Caldicott Guardian in relation to requests for records of deceased individuals.

6. Charging Fees for Access

6.1 The requester will be advised of any fees as soon as possible after the request is received and this will be payable before the request is further processed.

6.2 The General Data Protection Regulation (EU) 2016/679 removes the ability to charge fees for fulfilling subject access requests (unless manifestly unfounded or excessive) and tightens the statutory timeframe for completing a request to one calendar month (although the 21 calendar day target still applies to requests within the NHS).

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the CCG may either charge a reasonable fee (taking into account the administrative costs of providing the information or communication or taking the action requested) or may refuse to act on the request.

7. Access Requests for Minors

7.1 A child may make a subject access request in relation to their own personal data; as from the age of 13 they are normally considered competent enough to do so.

7.2 Those with parental responsibility for a child under 13 years may make an access request on their behalf but the information holder must consider whether it is in the best interests of the child to disclose information held.

8. Access Requests for those who lack capacity to consent

8.1 In certain circumstances a person acting as an advocate can seek access to personal information in so far as it is necessary or relevant to their role. This includes:

- Persons appointed by the Court of Protection
- Persons holding a registered Power of Attorney for specified purposes
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005

9. Third Party Requests for Access to Personal Data

9.1 There are a number of organisations concerned with law enforcement, crime prevention, fraud and taxation who have a right to request information from NHS Organisations under the provisions of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act. These requests should be

dealt with on an individual basis which balances the public interest against the confidentiality rights of the subject.

9.2 Any request should be authorised by an appropriately senior enforcement officer (an Inspector of Police or equivalent rank in other services) and should be accompanied by sufficient information to enable an informed decision to be made either by the Caldicott Guardian (in the case of patient related records) or Data Protection Officer. To state a 'serious crime' as the reason for a disclosure request is not sufficient and more detail must be provided.

9.3 The Coroner may request access to medical or staff records and is deemed to be acting in the public interest. Guidance and further information is available from the Information Governance Alliance.

9.4 NHS Wakefield CCG should take a pro-active approach to the sharing of information relevant to the safeguarding of children and vulnerable adults.

9.5 A number of other organisations including the Health and Safety Executive, Health Service Ombudsman and the Care Quality Commission may have rights of access in relation to enquiries being conducted. Advice should be sought from the Information Governance Team in the first instance. They will then liaise with the Caldicott Guardian or DPO as appropriate.

9.6 Follow any locally agreed Information Sharing Protocols and national guidance.

9.7 Information may be shared with Local and National Counter Fraud Specialists in relation to actual or suspected fraud in the NHS. The Data Protection Officer must be satisfied there is an appropriate lawful basis for the disclosure.

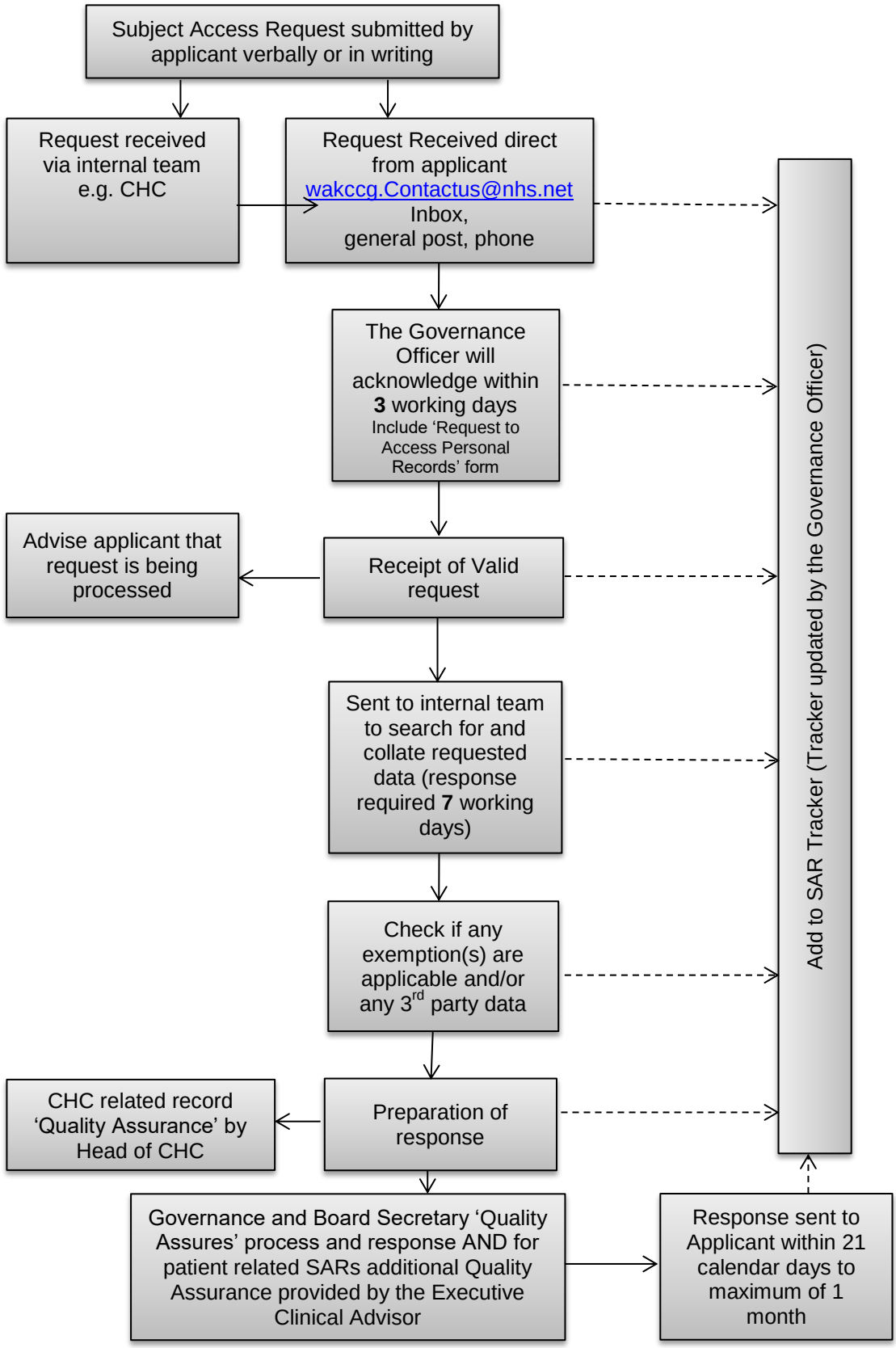
9.8 Personal information held by the CCG but originating from other organisations should be included unless such data is exempt or contains data regarding individuals other than the data subject.

10. Access to Corporate Information

10.1 NHS Wakefield CCG is a public authority and is subject to the provisions of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. Personal Data is usually exempted from public disclosure but in certain circumstances some personal data may be disclosed in the public interest but still subject to the individual's rights under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act.

11. Procedure

11.1 Procedural Flow Diagram



This section should be read in conjunction with the Checklist in **Appendix A.**

11.2 Receipt of an Access Request

- Discuss with the appropriate lead for access requests (Governance and Board Secretary).
- Check that the request relates to personal data of a type likely to be held by NHS Wakefield CCG.
- Consider whether the requester has supplied sufficient information to identify the data required, if not seek clarification before processing further.
- Consider whether you have sufficient evidence of identity of either the subject themselves or a third party authorised to act on their behalf.
- In the case of a third party, consider whether they meet the legal criteria to make a request and whether they have supplied evidence to that effect (for example where appropriate written consent from the individual).
- Consider whether the request is likely to be subject to a fee (see Section 6).
- Record the request in the subject access request tracking database. Include the date of receipt and due date for a reply.
- Arrangements should be in place for the safe and secure storage of access requests and responses with appropriate limited access provision. The Governance Officer will maintain a central file of subject access requests and responses.

11.3 Acknowledgement of request

- If the request meets the criteria above send an acknowledgement letter advising the requester of the expected timescale for a response to be provided.
- If further clarification, information, documentation or fees are required then request these as soon as possible.
- Make a record of your actions on the checklist.
- If the CCG does not hold the information, notify the requester in writing as soon as possible (no later than one month) and give advice and assistance where possible as to the location of the record.
- A template acknowledgement letter is provided at **Appendix C**.

11.4 Establishing Identity

- To help establish identity the application must be accompanied by photocopies of **two** official documents which between them clearly show the data subjects **name, current postal address, date of birth and signature**, for example: Birth Certificate, Local Authority provided bus pass, driving licence, passport, medical card, bank statement, utility bill, rent agreement. Ideally, one of the proofs should be a photographic identity document such as passport or driving licence.

11.5 Collating the data

- Consider where the information may be held and ask the relevant staff to conduct a search within the parameters of the request details.

- Ensure both electronic and manual filing systems are considered along with email, digital records, CCTV Images, telephone recordings and other media options.
- There is no exemption for potentially embarrassing information to be redacted or for the removal of personal comments from records. It is a criminal offence to alter, block or destroy information after receipt of a Subject Access Request.
- Information must be in an intelligible form and explanations should be provided for pseudonyms, abbreviations etc.

11.6 Potential Redactions or Refusals

- **All clinical data should be reviewed by a clinician** and consideration should be given to redacting any information likely to cause serious harm to the mental or physical health of any individual.
- Information supplied by or relating to third parties e.g. family members should usually be redacted.
- Data and information held from other agencies may be disclosable but should be discussed with the originating body first.
- Any information subject to Legal Professional Privilege should not be disclosed.
- Information should not be disclosed where there is a statutory or court restriction on disclosure e.g. adoption records.
- References written for current or former employees are exempt (but not those received from third parties).
- In the case of deceased records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential.
- A personal record may also contain reference to third parties and redaction should be considered by balancing the data protection rights of all parties.

11.7 Responding to the Request

- Check any fees have been received or additional supporting documentation requested at the time of acknowledgement.
- Send a holding letter with an explanation if it seems likely that the target date will be breached.
- Send the response to the requester explaining the information supplied.
- **Response letters must be approved by the Governance and Board Secretary (Information Governance Lead).**
- Make a record of the response, including any redactions or exempted information and ensure that you have a clear record of documents disclosed including copies of any redacted documents.
- Ensure that the requester is advised of his right to complain about the response given to his request and the way in which he can do this.
- Be prepared to facilitate a meeting to explain the records if necessary.
- Ensure the correspondence is suitably secure. Seek guidance from the IG Team in relation to secure transfer of responses.

11.8 Request to access legacy personal information

- Inform the requester that the CCG does not hold the requested information and provide assistance where possible to inform the requester where to direct their request.
- Legacy contact information:

  Reviews & Information Team
  Legacy Management Team
  Department of Health
  Skipton House
  80 London Road SE1 6LH
  Email: reviewsandinformationteam@dh.gsi.gov.uk

11.9 Summary of procedure

- Determine if it is a subject access request
- Confirm the requester's identity
- Ensure that sufficient information has been provided to identify the desired records
- Record the request
- Is personal information held on this person?
- Inform the applicant if the request has been deemed manifestly unfounded or excessive and any fee that would be charged for administration
- Will the personal information change (i.e. routine amendments to records) from receiving to responding to the request?
- Remove any 3rd party information where appropriate to do so
- Is some or all of the personal information exempt from the duty to comply with the subject access request?
- Explain any codes, complex terms and/or abbreviations as part of the subject access response provided
- Ensure a health professional checks the record(s) prior to disclosure
- Keep a record of the exact information provided to the requester
- Monitor to ensure the timescale for responding is met

12. References

This procedure is in place to ensure the organisation's compliance with legislation and guidance including, but not limited to, the following:

- A Guide to Confidentiality in Health and Social Care (NHS Digital)
- Access to Health Records Act 1990 (where not amended by the Data Protection Act 1998)
- Access to Medical Records Act 1988
- Audit & Internal Control Act 1987
- Caldicott 2 Principles –To Share or Not to Share? The Information Governance Review April 2013
- Children Act 1989 and 2004
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Coroners and Justice Act 2009

- Crime and Disorder Act 1998
- Data Retention and Investigatory Powers Act 2014
- Digital Economy Act 2017
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- General Data Protection Regulation (EU) 2016/679 and Data Protection Act
- Health and Social Care Act 2012
- Human Rights Act 1998
- Mental Capacity Act 2005
- NHS Act 2006
- NHS Care Records Guarantee for England
- Public Records Act 1958
- Records Management Code of Practice for Health and Social Care

13. Associated Documents

The procedure should be read in conjunction with the organisation's information governance policies:

- Information Governance Policy and Framework
- CCG Records Retention Schedule
- Confidentiality and Data Protection Policy and Procedure
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy (incorporating Network Security)
- E-Communications and Social Media Policy and Procedure
- Integrated Risk Management Framework
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy and Procedure
- Anti-Fraud, Corruption and Bribery Policy
- Whistleblowing Policy

And their associated procedures (including but not limited to):

- Interagency Information Sharing Protocol
- Data Protection Impact Assessment and Information Governance Checklist
- Safe Haven Guidelines and Procedure
- Confidentiality Audit Procedures

Appendix A

Subject Access and Access to Health Records Procedure Request Checklist

This checklist should be completed for each new request and should be read in conjunction with the Subject Access Request and Access to Health Record Request Procedure				
1	**Receipt of Request**	**Check**	**Date**	**Comments**
1.1	Is this a request under GDPR/DPA (or Access to Health Records Act 1990)?	☐		
1.2	Allocate a Subject Access request number	☐		
	Set up a secure file for all documents	☐		
	Date stamp all documents and correspondence.	☐		
2	**Identify Data Subject and Obtain Authorisation**			
2.1	Is the request valid?	☐		
	• Sufficient information to identify the data subject	☐		
	• Sufficient information to locate required data	☐		
	• Approval of IG Lead where third party request has been received	☐		
2.2	Send acknowledgement with appropriate form	☐		
	• To establish authorisation of data subject	☐		
	• To inform of fees, only if manifestly unfounded/excessive (evidenced admin cost)	☐		
	• Is the request made by the data subject	☐		
	• Or representative	☐		
	• Is authorisation attached	☐		
2.3	If the data subject is a child are they capable of making a request on their own behalf?	☐		
	If not, are the parents / guardians acting it in the best interest of the child? (check with health/social care professional)	☐		
2.4	Has the request been deemed manifestly unfounded or excessive? If so, please specify the admin cost being charged.	☐		
3	**Receipt of Valid Request**			
3.1	When request is valid:	☐		
	• Raise invoice (manifestly unfounded/excessive requests only)	☐		
	• Check fee has been paid (if applicable)	☐		
	• Record date and start to monitor the **21** calendar days to max **one month**	☐		
	• Send an acknowledgement to the data subject that the request is being processed	☐		
4	**Review of Information**			
4.1	Check if an exemption is applicable	☐		
4.2	Check third party identification and remove where necessary (consent not given)	☐		
4.3	Check information is accessible:	☐		
	• Check for intelligibility	☐		
	• All codes must be decoded	☐		
5	**Issue to Data Subject**			
5.1	If no problem with release of Data:	☐		
	• Request that the data subject or their representative collects the information	☐		
	• Information is sent Special Delivery/Guaranteed	☐		

	delivery to the data subject or their representative			
	• Ensure written response is approved by IG Lead	☐		
5.2	If information has been withheld under exemptions send out what is allowed to be disclosed and/or arrange an interview (if necessary) between health or social care professional and data subject to discuss the issues.	☐		
	If there is a delay send a holding letter	☐		
6	**Completion**			
6.1	Keep copies of all requests securely	☐		
Comments: Log of any calls, emails, post, and personal visits had in relation to this request. Please record time, date and initial any comments. Any delays should also be explained below.				

This request has been actioned by:

Name _____

Designation _____

Location _____

Date _____

Appendix B

Request to Access Personal Records

PRIVATE AND CONFIDENTIAL

Subject Access Request
General Data Protection Regulation (EU) 2016/679 and Data Protection Act

The form should be filled out in block capitals or in type.

Please note for health records requests: NHS Wakefield CCG is a commissioning organisation and not a healthcare provider. Health records will be held by the healthcare providers who you would need to contact directly to request records (contact details are shown in section 6 of this application form for local providers.

Section 1: Details of person whose records are being requested

Surname:	
Former Surname:	
First names:	
Title:	**Mr/Mrs/Ms/Miss**
Date of Birth:	
NHS Number:	
Current Address:	
Former Address : (if applicable)	

Section 2: Applicant details (if making a request on behalf of the person above)

Name:	
Address:	
Relationship to person in section 1:	

Section 3: Further Information

Please try and tell us what specific information you wish to see and provide as many details as possible so that we can identify your records as quickly as possible e.g. dates, department, location

Section 4: Consent

Please tick **one** of following boxes and sign below:

I confirm I am the person mentioned in section 1 and I require access to my personal records.	☐
I confirm I am the person mentioned in section 1 and I authorise the release of copies of my personal records (described in section 3) to the person mentioned in section 2.	☐
I confirm that I am the person mentioned in section 2 and I have parental responsibility for the child in section 1.	☐
I confirm I am the person mentioned in section 2 and have been authorised to an act as an agent/power of attorney for the patient in section 1.	☐

Name:	PLEASE WRITE NAME IN CAPITALS
Signature:	
Date:	

Section 5: Evidence

Evidence of the patients and/or the patient's representative identity will be required; this will require **two** items of documentation (one of which should contain a photograph), examples of which are given below:

Type of applicant	**Type of documentation required**
An individual applying for their own records.	Two copies of identity required e.g. copy of birth certificate, passport, driving licence, medical card etc. Together, these must clearly show your name, current postal address, date of birth and signature
Someone applying on behalf of an individual.	One item of proof of the patient's identity and one items of proof of the patient's representative identity (examples above).
Person with parental responsibility applying on behalf of their child.	Copy of birth certificate, correspondence addressed to the person with parental responsibility relating to the patient.
Power of attorney/agent applying on behalf of an individual.	Copy of court order authorising power of attorney/agent plus proof of the patient's identity (examples above).

Please return the form to the:
Governance Department
NHS Wakefield Clinical Commissioning Group
White Rose House
West Parade
Wakefield
West Yorkshire
WF1 1LT

Please note:

- A completed form will contain confidential information, therefore where sending by letter - to provide more security during the transit of a letter it is advisable that the form is sent in an envelope marked "PRIVATE AND CONFIDENTIAL".

- If you are intending to send the form via email, the transit of the email (if sending from a home email address or company email) will in most cases not be secure and therefore the security of the information cannot be assured.

Section 6: Contact details for Health Records (Health providers)

Please note: this application form is for the NHS Wakefield CCG only. The NHS organisations below all have their own application process.

Acute/secondary/hospital care The Mid Yorkshire Hospitals NHS Trust

Records held by Acute Trusts (secondary care provider) include outpatient attendances; inpatient stays, day care, Accident and Emergency attendance all which usually take place at the hospital. Requests for these types of records should be made to the acute Trust itself. The Mid Yorkshire Hospitals NHS Trust includes Pinderfields, Pontefract and Dewsbury hospital sites.

The contact details are:
The Mid Yorkshire Hospitals NHS Trust
Pinderfields Hospital
Aberford Road
Wakefield
WF1 4DG

Primary care (GP records)

Records from visits to the GP or practice nurse will be held by the practice itself. Requests for these types of records should be made direct to the practice.
NHS Choices website

Mental Health South West Yorkshire Partnership NHS Foundation Trust

The mental health trust provides specialist mental health and learning disability services, their contact details are:

South West Yorkshire Partnership NHS Foundation Trust
Fieldhead
Ouchthorpe Lane
Wakefield
WF1 3SP
www.southwestyorkshire.nhs.uk/

Appendix C

Draft Acknowledgement Letter

PRIVATE AND CONFIDENTIAL

SAR Ref: <Unique ID>

DATE

Name
Address

Dear Mrs/Ms/Miss/Mr XXXXXX

Access Request under the General Data Protection Regulation (EU) 2016/679, Data Protection Act or Access to Health Records Act 1990

Thank you for your request for information under the XXXXXX received on XXXXXX This letter is to acknowledge receipt of the request addressed/made verbally to NHS Wakefield CCG on XXXXXX. *In order to process your request I would be grateful if you could complete and return the attached form.*

On receipt of the completed form we would expect to forward a response to you within 21 days dependent upon whether any clarification is needed and/or whether fees are to be charged. In such circumstances, the CCG will notify you as soon as possible of any fees which may be due.

Under the legislation there may be restrictions which the CCG is obliged to apply but these will be explained to you in our response.

Yours sincerely

[name of signatory]

SECTIONS IN ITALICS TO BE DELETED IF REQUEST IS ALREADY ON FORM OR IF IT IS COMPLETE IN ANOTHER FORMAT

Appendix K

Guidance Relating to Document Retention and Court Proceedings

1. Introduction

If staff become aware that there is a possibility of court proceedings against the CCG, they must alert the Governance and Board Secretary or the Associate Director of Corporate Affairs and the Chief Officer or Chief Finance Officer/Deputy Chief Officer so that appropriate action can be taken.

2. Duty of candour

In judicial review proceedings, the parties are required to ensure that all relevant information and facts are put before the court. This is known as the 'duty of candour' and includes all material facts or information which either support or undermine a party's case. Before the claim form is filed, the parties are expected to work to properly identify and understand the issues in dispute and share information and relevant documents that are properly necessary for that purpose. The courts expect that throughout the proceedings the parties will continue to communicate constructively and effectively.

Upon receipt of the claim form and accompanying grounds of claim and evidence, if not before, defendant public authorities owe a high duty to make full and fair disclosure of relevant material and provide full and accurate explanations of relevant facts and reasoning. They must act with due diligence in investigating what material and information are available and disclosing that which is relevant or assists the claimant.

Disclosure is not generally ordered in judicial review proceedings because the courts trust public authorities to discharge the duty of candour, but specific disclosure (or cross examination of witnesses) may exceptionally be ordered, particularly where it transpires that the duty has not been discharged, or matters of fact must be established before a claim can be resolved. Sanctions for failures to discharge the duty of candour may also include the refusal of relief and the imposition of costs sanctions.

3. Document retention – the key points are as follows:

a. Do not destroy documents.

Now that litigation is contemplated, please do not delete any documents in relation to this matter, and please suspend any routine document destruction policies you have in place. It will be necessary to err on the side of caution and preserve anything that relates to this potential claim even if it does not appear immediately pertinent.

You will be required to search for and provide relevant documents if and when proceedings are on foot. If we get to Court, our list of disclosed documents will need to state what has happened to any documents that have been lost or destroyed. A suggestion that potentially important documents may have been lost or destroyed after the proceedings began could be very damaging to our case. The court rules expressly require you to be notified, as soon as litigation

is contemplated, of the need to preserve disclosable documents, including electronic documents that would otherwise be deleted in accordance with a document retention policy or in the ordinary course of business. Failure to comply with this could lead to the court drawing adverse inferences.

b. Do not create documents (or annotate or amend existing documents).
It is very important that you do not create any new documents that we might have to disclose to an opponent in light of the duty of candour (as described below), that could damage our case. If in doubt please check before creating any document.

Some documents that are created may be protected by legal privilege, which will mean that they do not need to be disclosed. However, you will need to monitor carefully any communications about this matter, whether internal or external. This particularly includes communications between, or involving, those who are not involved in making decisions about the way in which the litigation should be conducted. It may be appropriate for such people not to communicate about the dispute at all, unless they are instructed to do so. In any event, you should take particular care when using email.

At this point, you should not amend, or in any way annotate, existing documents. Documents containing any relevant annotations will be treated as separate documents and may need to be disclosed even if the original document was not disclosable. Informal annotations, in particular, can be prejudicial to the case of the party that is obliged to disclose them.

c. Do not ask any third party to send you documents.
There are certain documents that the CCG may not have in its possession, and may not have the legal right to possess, inspect or copy (for example, the working papers of third-party professional agents, such as other firms of solicitors, or accountants). Those third-party documents will not be disclosable, unless they come into the CCGs' possession (although some documents may already been deemed to be within the CCGs' control, if held on their behalf).

It is therefore extremely important that you do not ask any third parties to send you documents that may relate to the dispute at this point, unless a lawyer has the opportunity to assess the documents they propose to send.