NHS
West Essex
Clinical Commissioning Group

Information Lifecycle Management Policy

Policy Reference: IG04

Brief Summary:
This policy, procedure and strategy sets out the intentions of the Clinical Commissioning Group in relation to managing the lifecycle of information through each stage of its existence from creation to destruction. It will detail the processes which all staff must embed within their working practices to ensure that information is at minimal risk of being compromised.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	01/02/2013	Draft	New Document	NHS Central Eastern Commissioning Support Unit Information Governance Team
1.0	14/02/2013	Final	Approved by West Essex CCG	NHS Central Eastern Commissioning Support Unit Information Governance Team
1.1	17/10/2014	Draft	Changes in guidance and reporting structure necessitates policy review	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.2	18/12/2014	Draft	Key contacts added	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.3	05/03/2015	Final	Approved by West Essex CCG	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG's Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019
Responsibility for Review	CCG's Information Governance Team
Audience	All CCG officers and staff (includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

This policy relates to NHS West Essex Clinical Commissioning Group (the CCG). Information Lifecycle Management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation to destruction. Records Management forms part of the CCG's Information Lifecycle Management and is the process by which the 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.

The Records Management: NHS Code of Practice has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

Records within the NHS can be held in paper or electronic form. All NHS organisations will have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Record Guarantee.

The CCG's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision making, protect the interests of the CCG and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in uniform and equitable ways. They are a valuable resource because of the information they contain and support the delivery of high quality evidence based healthcare. Information has most value when it is accurate, up to date and accessible when needed.

The CCG has written this Information Lifecycle Management Policy and is committed to ongoing improvement of records management functions as they believe a number of organisational benefits will be gained from doing so, including:

- Better use of physical and server space;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards;
- Reduced costs and
- Archiving and Disposal.

The CCG also believes that internal management processes will be improved by the greater availability of information that will accrue through the recognition of records management as a designated corporate function.

This document sets out a framework to enable staff responsible for managing the CCG's records to develop specific policies and procedures to ensure that these are managed and controlled effectively and, at best value, commensurate with legal, operational and information needs.

It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy.

2. Purpose

The aims of our Records Management System are to ensure that:

- **Records are available when needed** - from which the CCG is able to form a reconstruction of activities or events that have taken place;
- **Records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use and that the current version is identified where multiple versions exist;
- **Records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process and how the record is related to others ;
- **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 disclosures 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 they are required;
- **Records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value;
- **Staff are trained** - so that all staff are made aware of their responsibilities for recordkeeping and management.

3. Scope

This policy relates to all records held in any format by the CCG. These include:

- All administrative records (for example personnel, estates, financial / contracts and accounting and those associated with complaints);
- All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers and so on);
- Computer databases, output and disks and all other electronic records;
- Material intended for short term or transitory use, including notes and spare copies of documents;
- Meeting papers, agendas, formal and information meetings including notes taken by individuals in note books, bullet points and e-mails;
- Audio and video tapes, cassettes and CD ROMs

This list is not exhaustive.

4. Definitions and terms

Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- Record creation;
- Record keeping;
- Record maintenance (including tracking of record movements);
- Access and disclosure;
- Closure and transfer;
- Appraisal;

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

In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the CCG in the transaction of their business or conduct of affairs and kept as evidence of such activity'.

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

5. Roles and Responsibilities

Accountable Officer for NHS West Essex Essex CCG

The Chief Officer of the CCG is the Accountable Officer and has overall responsibility for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available when required.

Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of CCG Senior Information Risk Owner (SIRO) is held by the Director of Finance, Contracting and Performance. The SIRO is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy. The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk and for guaranteeing the CCG Governing Body is adequately briefed on information risk issues.

Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service-users information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to do so and for advising on options for lawful and ethical processing of information.

All Staff

Under the Public Records Act every member of staff is responsible for the records they create, receive and use in the course of their duties. Staff should ensure that they comply with this policy at all times and report any breaches through the appropriate incident reporting channels.

Irrespective of its format, all staff must ensure that the following principles are applied to all records created:

- A consistent definition should be adopted to the creation, use, storage, retrieval, archiving, and disposal of records.
- All staff should ensure records are stored within a filing structure that reflects the CCG's business functions. Records must not be retained, disseminated or duplicated unnecessarily.

- All staff should ensure that records are disposed of by the authorised member of staff and this must be done in accordance with the Records Management Retention and Disposal Schedules.
- Staff should keep complete and accurate information of all records, activities and transactions and ensure records are captured and managed within the appropriate information and records management systems.
- Staff should ensure e-mail is only used a source transmission and not for storage.
- Staff MUST not store information in individual filing systems or on hard drive (that is 'my documents 'or 'desktop').

Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrators (IAAs)

Information Asset Owners can appoint an Information Asset Administrator (IAAs) to support in the management of records with their department / directorate.

Information Asset Administrators are responsible for:

- Ensuring that all staff within their directorate / department are fully aware of their responsibilities and legal obligations for records management in compliance with policy
- Conducting regular audits of records management functions
- Reporting policy breaches using the organisation incident reporting mechanism
- Ensuring that effective and relevant file management systems are in place for information held within their directorate / department.

Head of Information Governance

The Head of Information Governance is responsible for the overall development and maintenance of all records management practices throughout the CCG, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

6. Legal Professional Obligation

All NHS records are public under the Public Records Acts. The CCG will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice and any new legislation affecting records management as it arises, in particular:

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice and
- The NHS Care Record Guarantee

7. Creation and Management of Records

Creation

Records are created to support the day-to-day running of the CCG's business. A record is created when it meets the legal requirement defined above.

Records created by staff should be arranged in a recordkeeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

Policy on procedural documents

Certain documents such as policies and procedures undergo a consultation process with numerous drafts prior to approval. It is therefore necessary that reference is made to the document version and this is revised with each review using version controls for the management of multiple revisions to the same document to enable the author and other users to identify one version of a document from the other. These include:

- Keeping successive drafts of the document to provide adequate evidence of the process for example substantial changes during the development of policy.
- Inserting 'Draft' watermarks to indicate the status of the version.
- Following numbering system by using number with points to reflect minor and major version changes for example 0.1, 0.2 for minor changes.
- Changing the final version to v1.0 when the document has reached its 'Final' version and continue with 1.1, 1.2 for minor changes to the first version.

Version number	Summary of changes	Author	Date
0.1	Initial draft shown to line manager	Louis Lane	01/02/2014
0.2	Includes comments from line manager – section 2	Louis Lane	08/02/2014
0.3	Includes comments from the workgroup section 2,5,6	Louis Lane	01/03/2014
0.4	Correction of grammar and spelling – section 2, 8	Clark Kent	10/05/2014
0.5	Amendment of section 12 to reflect a procedure change	Louis Lane	15/09/2014
1.0	Change of business unit name and published on the Intranet	Kate Moss	06/01/2015

Please see Appendix A for Checklist for Policy Approval

Referencing and naming conventions

A naming convention is essential for all corporate records. Records should be easily accessible and understandable to staff across the organisation. Corporate records need to follow an agreed naming convention using a systematic approach, for example it should be:

- easily understood by the staff that create and access records
- alphanumeric:
- Beginning with key letters or words identifying the directorate;
- Identifying the department, followed by the business activity;
- Identifying the document name
- Including the initials of the author/creator
- Including a version number
- Identifying the year of creation

Filing structure

A clear and logical filing structure that aids the retrieval of records must be used. The filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible, the names allocated to files and folders should allow ‘intuitive filing’. Filing of the primary corporate record to local drives on PCs and laptops is not permitted.

The agreed filing structure will also help with the management of the retention and disposal of records.

Shared drives

It is important to consider the content of a document when using this option. Where access to the document is to be limited, the creator of the document must ensure that the record is located in a restricted area on the shared drive.

Staff should ensure that any personal folders are not created on their department's shared drive. Folders created on a shared drive should title the project name or intents.

Records should not be saved on local / personal drives or personal computers.

Scanning

For the purpose of business efficiency and adapting to paperless innovation, the CCG will consider the option of scanning paper records into electronic format; this will facilitate issues with storage space. Where this is proposed, the following factors will be taken into consideration:

- The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;
- The need to consult in advance with the local place of deposit or the National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and
- The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically'

Standards for a Scanned Image

Images must adhere to the following standards;

- Every image must be a true representation of the original document
- All text must be legible.
- The patient / staff member associated with the document must be clear on the scanned image.
- All images received from an external source must be date stamped when received, before scanning into electronic form. This must be clear on the scanned document.
- There must be an audit trail on the system of the date and time when the image was scanned into the system.
- There must be a completed audit trail of information detailing who scanned and saved the image into the system, inclusive of time and date.

- The image should be saved to a suitable agreed resolution to ensure quality.
- An audit trail must be kept detailing destruction of any documents. The best practice process would be to retain the original information with the scanned image.

For a process map to scan a document received via post, please see Appendix B

Standards for an Adobe Image

Documents may be converted into an ‘Adobe’ image and saved like a scanned image. However, images must adhere to the following standards:

- Every image must be a true representation of the original document
- All text must be legible
- The patient / staff member associated with the document must be clear on the image
- There must be an audit trail on the system of the date and time when the image was saved into the system.
- There must be an audit trail of who saved the image into the system.
- The image should be checked before it is saved to ensure quality.

Tracking and Tracing

Tracking and tracing procedures implemented must enable the movement and location of records to be controlled. This will provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from, or returned to, its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

- the item reference number or identifier;
- a description of the item (for example the file title);
- the person, position or operational area / team who may have possession of the item;
- the date and time of movement that took place

Secure Transfer of Information & Protective Marking

It is important that when information needs to be shared, it is transferred and / or transported in a secure and efficient manner. There are many different methods of transferring information and it is vital that the most appropriate method is chosen, dependent on the type of information to be transferred.

For more information on methods of secure transfer, please see Appendix C.

New Government Security Classifications (published April 2014) have been implemented to assist in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect.

Details of classifications can be found on Appendix D.

Retention and Disposal

It is a fundamental requirement that all of the CCG's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the CCG's business functions**.**

The CCG has adopted the retention periods set out in the Records Management: NHS Code of Practice. The retention schedule will be reviewed as appropriate by NHS England.

Archiving

Once a record has ceased to be accessed regularly, for example if the member of staff has left the organisation or the record refers to a historic business activity, it is necessary for the practical operation of the organisation that this then should be archived to an alternative storage location.

The CCG has adopted the retention periods detailed within the NHS Code of Practice Annex D1 Health Records Retention Schedule and Annex D2 Business and Corporate (Non Health) Records Retention Schedule. See Appendices E & F.

The retention schedules detail the Minimum Retention Period for each type of record. Records, whatever the media, may be retained for longer than the minimum period, however this requires formal approval of the Information Governance Steering Group (IGSG). They should not however be retained for more than 30 years. Where a period longer than 30 years is required (for example to be preserved for historical purposes), or for any pre-1948 records, the National Archives should be consulted.

It should be noted that records containing personal information are subject to the Data Protection Act 1998. The 5th principle states that personal data should not be retained longer than is necessary.

If a particular record is not listed in the schedules the Information Governance Lead should be contacted for advice.

The Intranet

The Intranet is a web-based communication tool. It has been set up in a centralised location to enable staff to easily locate any materials that they may need. This is to help them carry out their duties or to generally find out more information on a particular subject.

Examples of information which should be published on the Intranet are:

- Policies, Procedures and Strategies
- Forms
- Contact Lists
- Minutes of Meetings
- General Information
- Newsletters

Examples of information which *should not* be published on the Intranet are:

- Confidential Information
- Patient / Personal Information
- Commercially Sensitive Information
- Incomplete Information for example. draft documents

Public Facing Website

Information that is intended to be made publicly available should be published through the Freedom of Information (FoI) Publication scheme located on the Public Facing Website. Requests for new content to be added should be made via the FoI Lead / Co-ordinator.

Examples of information which should be routinely published on the public facing website are:

- The CCG Annual Report
- Press Releases
- Up to date contact Information for the CCG
- Information about services provided by the CCG
- A list of the main categories of Information that have been most frequently requested via the FOIA
- A list of data sets requested previously under the FOIA

Examples of information which *should not* be published on the public facing website are:

- Person Identifiable Information of any description
- Confidential Reports
- Commercially Sensitive Information
- Incomplete Information for example draft documents, any information not approved or finalised

8. Success Criteria

The CCG Information Governance Action / Improvement Plan which includes Records Management will be monitored by the IG Team and reported to the Audit Committee.

A regular audit of records management functions will be undertaken by IAAs.

The audit will:

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

9. Audit and Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has a responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect it. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from this prompted by incident review, external reviews or other sources of information and advice.

10. Dissemination and Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

11. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

12. Related CCG documents

- Information Governance Policy
- Confidentiality & Data Protection Act Policy
- Information Sharing Policy
- Safe Haven Policy
- Information Security Policy
- Subject Access Request Policy & Procedure
- Information Risk Policy
- Freedom of Information Policy

Please see Appendix G for information of related Legal Acts

13. Equality and Diversity

NHS **West Essex** CCG recognises the diversity of the local community and those in its employment. The organisation aim to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need.

This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

14. Key Contacts within the CCG

Within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	Debbie.smith-shaw@nhs.net

Appendix A

Checklist for Approval of Policy

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

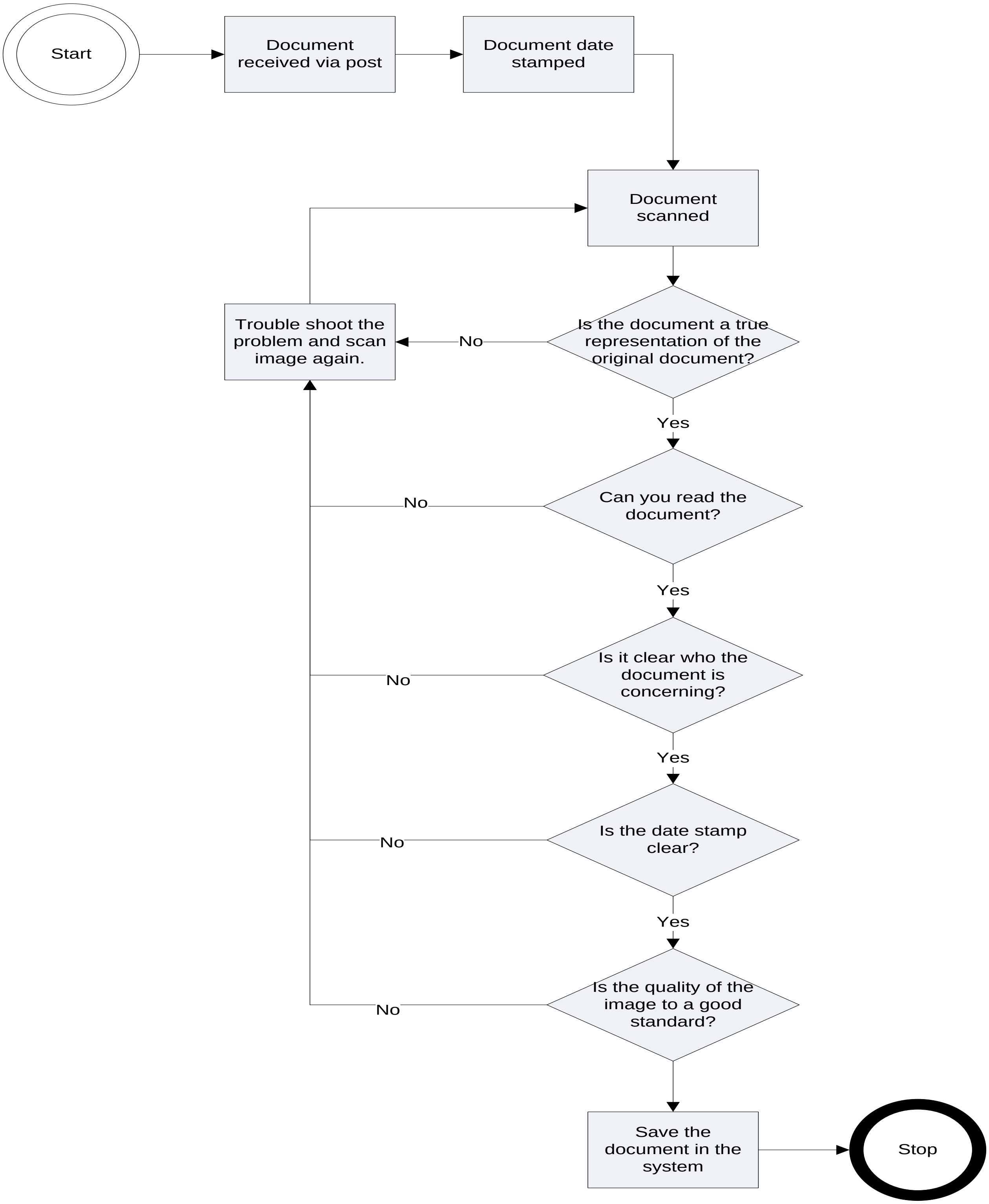
	Title of document being reviewed:	**Yes/No/ Unsure**	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?	YES	
	Is it clear whether the document is a guideline, policy, protocol or standard?	YES	
2.	**Rationale**		
	Are reasons for development of the document stated?	YES	
3.	**Development Process**		
	Is the method described in brief?	YES	
	Are people involved in the development identified?	YES	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	YES	
	Is there evidence of consultation with stakeholders and users?	YES	
4.	**Content**		
	Is the objective of the document clear?	YES	
	Is the target population clear and unambiguous?	YES	
	Are the intended outcomes described?	YES	
	Are the statements clear and unambiguous?	YES	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	YES	
	Are key references cited?	YES	
	Are the references cited in full?	YES	

	Title of document being reviewed:	**Yes/No/ Unsure**	**Comments**
	Are supporting documents referenced?	YES	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	YES	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	YES	
	Does the plan include the necessary training/support to ensure compliance?	YES	
8.	**Document Control**		
	Does the document identify where it will be held?	YES	
	Have archiving arrangements for superseded documents been addressed?	YES	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	YES	
	Is there a plan to review or audit compliance with the document?	YES	
10.	**Review Date**		
	Is the review date identified?	YES	
	Is the frequency of review identified? If so is it acceptable?	YES	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	YES	
12	**Equality Impact Assessment (EIA)**		

	Title of document being reviewed:	**Yes/No/ Unsure**	**Comments**
	Has an equality analysis been undertaken in preparation for this policy?	YES	
	Has the equality analysis been quality assured by the Equality and Diversity Group?		

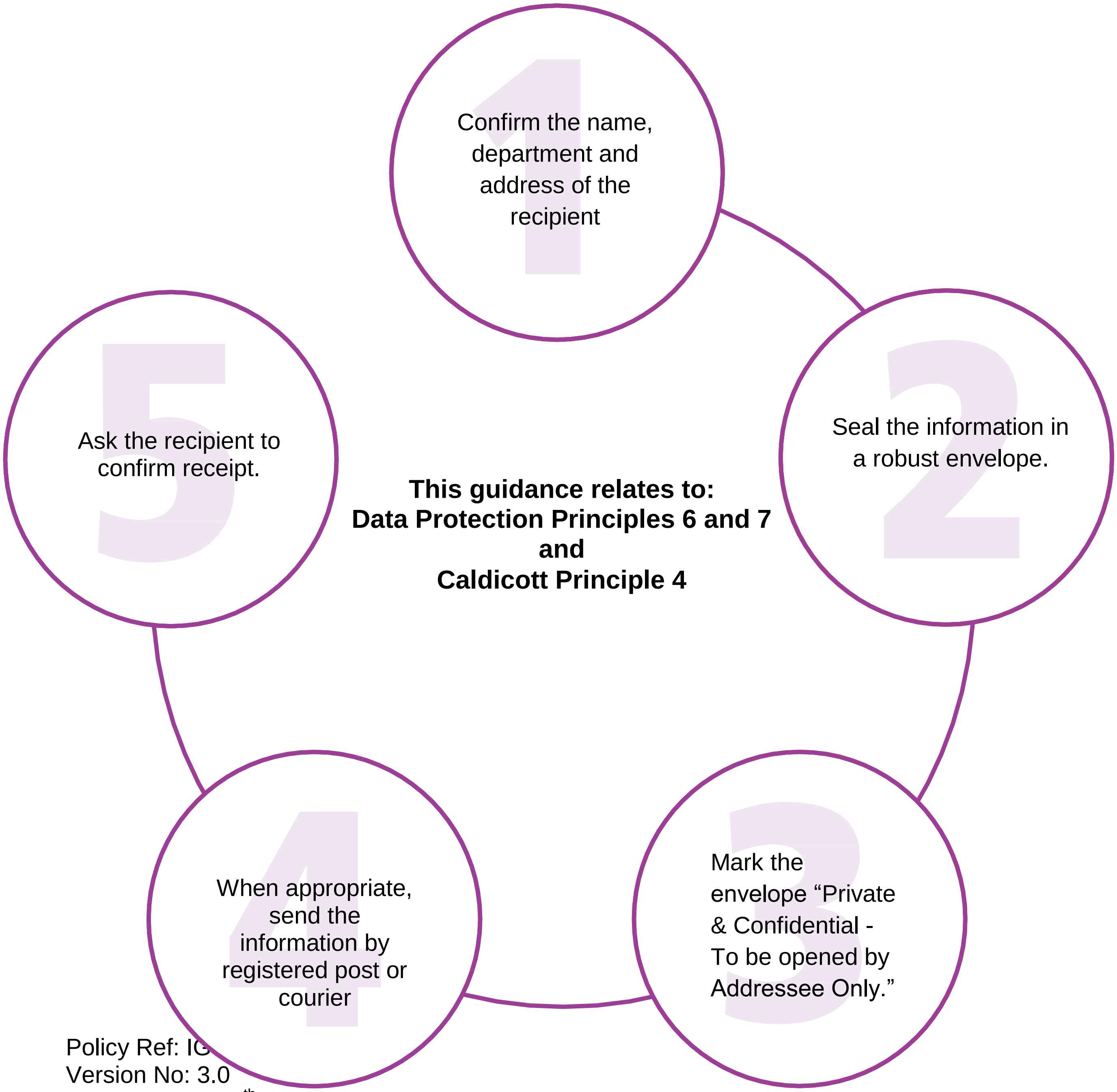
Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name		Date	
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name		Date	
Signature			

Appendix B: Process Map for Scanning a Document Received Via Post


Start
Document received via post
Document date stamped
Document scanned
Is the document a true representation of the original document?
No
Trouble shoot the problem and scan image again.
Yes
Can you read the document?
No
Yes
Is it clear who the document is concerning?
No
Yes
Is the date stamp clear?
No
Yes
Is the quality of the image to a good standard?
No
Save the document in the system
Stop

Appendix C: Methods of Secure Transfer

information by **POST**



1 Confirm the name, department and address of the recipient

2 Seal the information in a robust envelope.

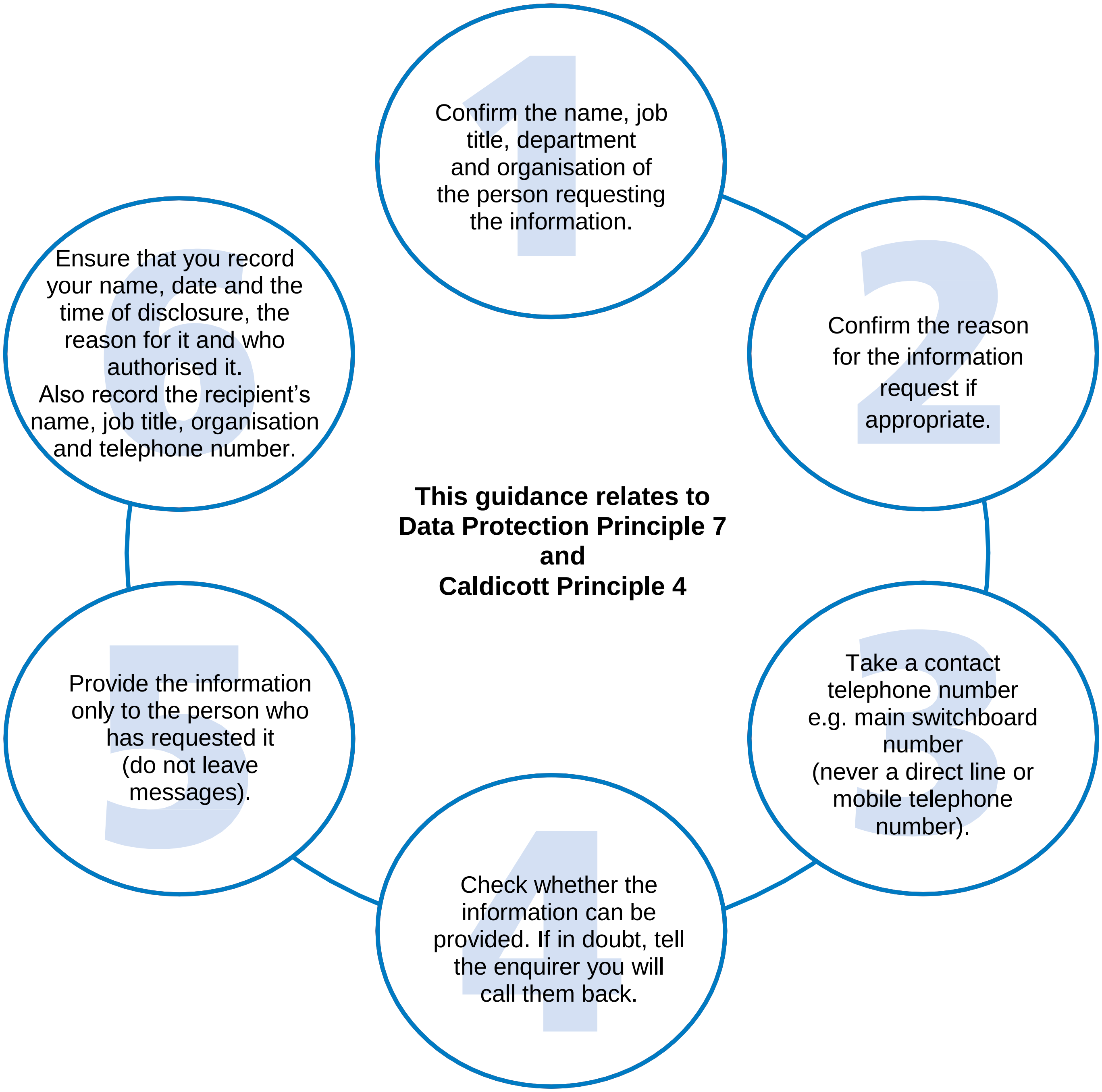
3 Mark the envelope “Private & Confidential - To be opened by Addressee Only.”

4 When appropriate, send the information by registered post or courier

5 Ask the recipient to confirm receipt.

This guidance relates to:
Data Protection Principles 6 and 7
and
Caldicott Principle 4

information by TELEPHONE



Confirm the name, job title, department and organisation of the person requesting the information.

Confirm the reason for the information request if appropriate.

Take a contact telephone number e.g. main switchboard number (never a direct line or mobile telephone number).

Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

Provide the information only to the person who has requested it (do not leave messages).

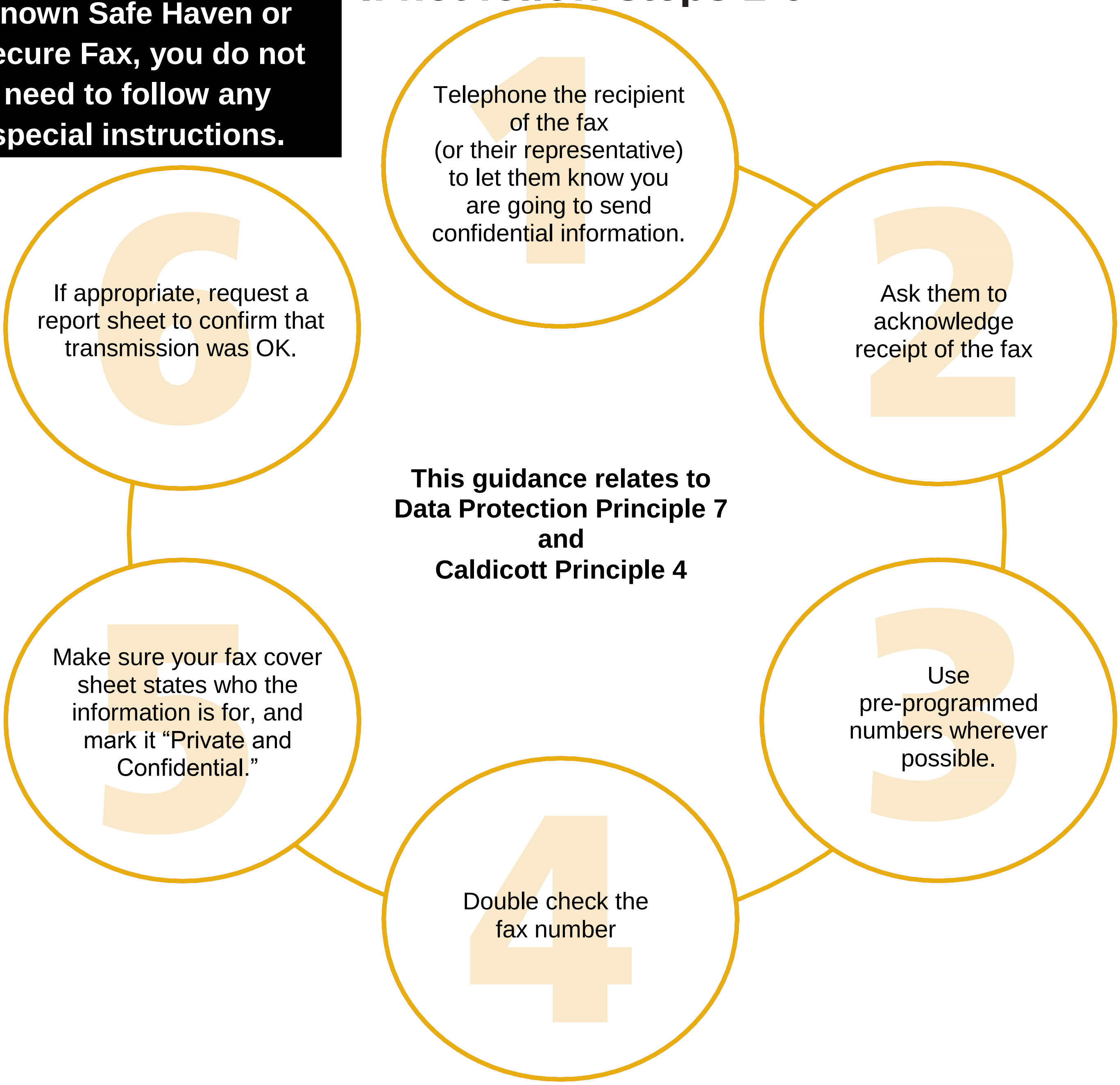
Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it.
Also record the recipient's name, job title, organisation and telephone number.

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

information by **FAX**

If you are faxing to a known Safe Haven or Secure Fax, you do not need to follow any special instructions.

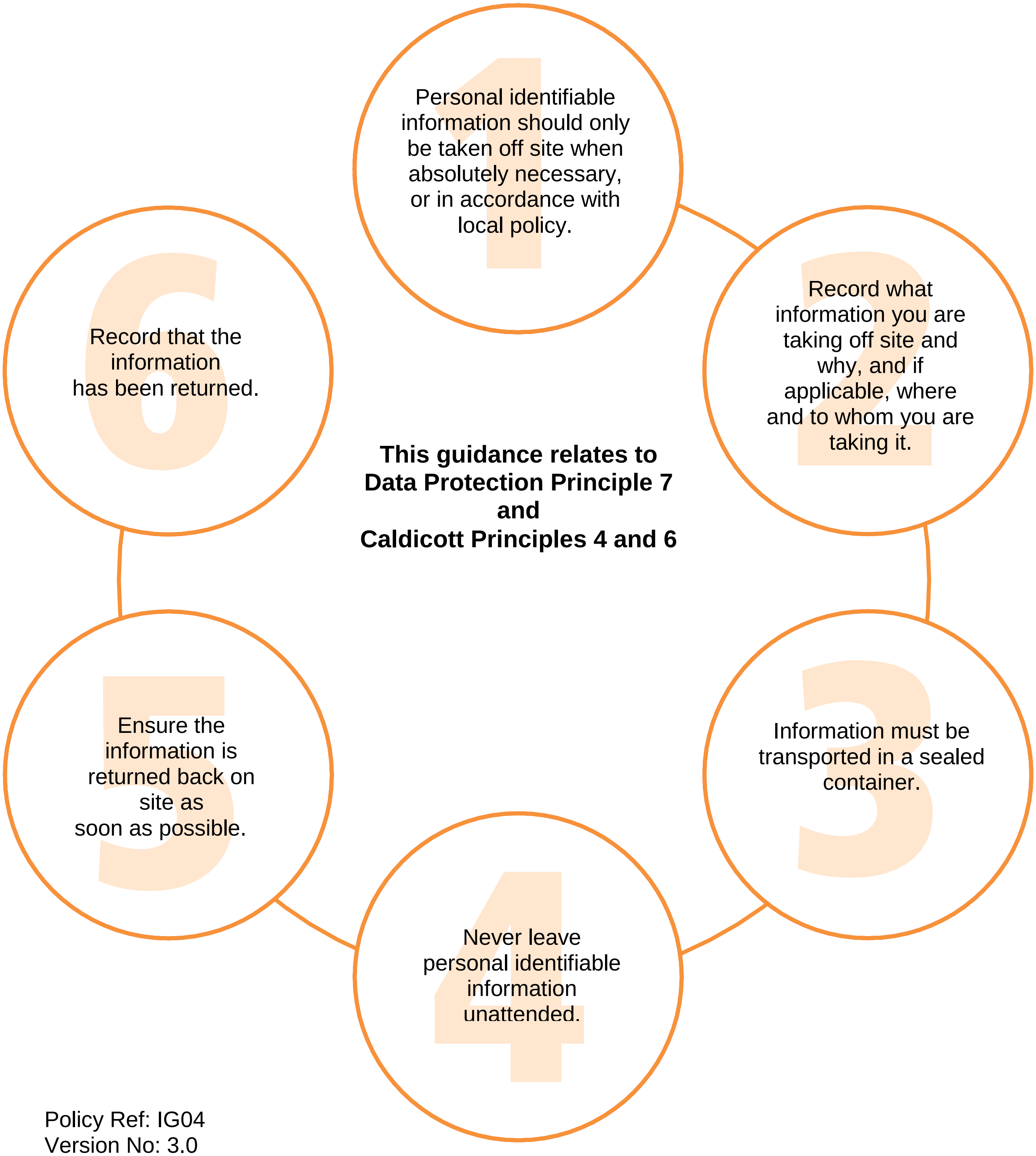
If not follow steps 1-6



1. Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information.
2. Ask them to acknowledge receipt of the fax
3. Use pre-programmed numbers wherever possible.
4. Double check the fax number
5. Make sure your fax cover sheet states who the information is for, and mark it “Private and Confidential.”
6. If appropriate, request a report sheet to confirm that transmission was OK.

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

Guidance for TRANSPORTING personal information



This guidance relates to Data Protection Principle 7 and Caldicott Principles 4 and 6

1. Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.

2. Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.

3. Information must be transported in a sealed container.

4. Never leave personal identifiable information unattended.

5. Ensure the information is returned back on site as soon as possible.

6. Record that the information has been returned.

Policy Ref: IG04
Version No: 3.0
Approval Date: 7th October 2016
Review Due: March 2019

Appendix D: Protective Marking Scheme

Classification of NHS Information - Marking Guidance for CCGs

ALL information the CCG collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works within the CCG (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any CCG information or data that they access, irrespective of whether it is marked or not.

New Government Security Classifications (published April 2014) have been implemented to assist you in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The new levels are;

<u>OFFICIAL</u>

Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. The CCG will operate exclusively at this level including the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

<u>SECRET</u>

Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well- resourced and determined threat actors and highly serious organised crime groups.

<u>TOP SECRET</u>

Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or

allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

There is no need to apply the new classification procedure retrospectively.

This simplified procedure will make it easier and more efficient for information to be handled and protected. The new procedure places greater emphasis on individuals taking personal responsibility for data they handle.

All information used by the CCG is by definition ‘OFFICIAL.’ It is highly unlikely the CCG will work with ‘SECRET’ or ‘TOP SECRET’ information.

Things to remember about OFFICIAL information:

1. Ordinarily OFFICIAL information does not need to be marked for non-confidential information.
2. A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but should have additional measures applied in the form of OFFICIAL- SENSITIVE.
3. This marking is necessary for person identifiable information and commercially sensitive information and is applicable to paper and electronic documents / records.
4. In additional to the marking of OFFICIAL-SENSITIVE further detail is required regarding the content of the document or record, that is OFFICIAL – SENSITIVE: COMMERCIAL

   Definition - Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG or a commercial partner if improperly accessed.

   Or

   OFFICIAL – SENSITIVE: PERSONAL

   Definition - Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

   Such documents / records should be marked with the caveat ‘OFFICIAL-SENSITIVE: COMMERICAL or SENSITIVE’ in capitals at the top and bottom of the page.

   In unusual circumstances OFFICIAL – SENSITIVE information may contain both Personal and Commercial data, in such cases the descriptor OFFICIAL – SENSITIVE will suffice.

NHS Confidential

The CCG has adopted the new government classification scheme for corporate information as it is an expectation from the DH for all arms length bodies (ALBs) to comply with. Our approach will satisfy any corporate communications with DH, other departments and ALBs. In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

How to handle and store OFFICIAL information;

EVERYONE is responsible to handle OFFICIAL information with care by:

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

How to handle and store OFFICIAL – SENSITIVE information;

All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, OFFICIAL-SENSITIVE:

PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules
- Always question whether your information may need stronger protection
- Make sure documents are not overlooked when working remotely or in public areas, work digitally to minimise the risk of leaving papers on trains and so on
- Only print sensitive information when absolutely necessary
- Send sensitive information by the secure e-mail route or use encrypted data transfers
- Encrypt all sensitive information stored on removable media particularly where it is outside the organisation's physical control
- Store information securely when not in use and use a locked cabinet / drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details
- Do not send to internet e-mail addresses for example Gmail, Hotmail and so on.
- Only in exceptional cases, where a business need if identified, should sensitive information be e-mailed over the internet, in an encrypted format, to the third parties. Contact the Corporate IG team for further advice
- The use of pin code for secure printing is both widely available and preferable way to manage the printing process

Table 1 – Descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL

Category	Definition	Marking
Appointments	Concerning actual or potential appointments not yet announced	OFFICIAL-SENSITIVE: COMMERCIAL
Barred	Where • there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or • disclosure would constitute a contempt of Court (information the subject of a court order)	OFFICIAL-SENSITIVE: COMMERCIAL
Board	Documents for consideration by an organisation's Board of Directors, initially, in private (Note: This category is not appropriate to a document that could be categorised in some other way	OFFICIAL-SENSITIVE: COMMERCIAL
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs	OFFICIAL-SENSITIVE: COMMERCIAL
Contracts	Concerning tenders under consideration and the terms of tenders accepted	OFFICIAL-SENSITIVE: COMMERCIAL
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date	OFFICIAL-SENSITIVE: COMMERCIAL
Management	Concerning policy and planning affecting the interests of groups of staff (Note: Likely to be exempt only in respect of some health and safety issues)	OFFICIAL-SENSITIVE: COMMERCIAL
Patient Information	Concerning identifiable information about patients	OFFICIAL-SENSITIVE: PERSONAL

Personal	Concerning matters personal to the sender and/or recipient	OFFICIAL-SENSITIVE: PERSONAL
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published)	OFFICIAL-SENSITIVE: COMMERCIAL
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.	OFFICIAL-SENSITIVE: COMMERCIAL
Staff	Concerning identifiable information about staff	OFFICIAL-SENSITIVE: PERSONAL

Appendix E: Clinical Record Retention Periods

Type of Record (Clinical)	Retention Period
A&E Records	8 years adult, 25th birthday child
Admission Books	8 years
Ambulance Records	10 years
Audiology Records	8 years adult, 25th birthday child
Birth Registers	2 years
Birth Notification	25th birthday of child
Cancer Care Records	8 years adult, 25th birthday child
Child Health Record	25th birthday of child
Clinical Audit Records	5 years
Clinical Psychology	20 years
Death Registers	2 years
Dental Records Including Study Models	11 years adult, 25th birthday child
Diaries	2 years after current year
Dietetic and Nutrition	8 years adult, 25th birthday child
District Nurse Records	8 years adult, 25th birthday child
DNA (Did Not Attend)	8 years adult, 25th birthday child
Electrocardiogram (ECG) Records	7 years
Endoscopy Records	8 years adult, 25th birthday child
Family Planning Records	10 years adult, 25th birthday child
GP Records	10 years after death or emigration
Health Visitor Records	10 years
Hospital Acquired Infection Records	6 years
Hospital Records Not Listed Elsewhere	8 years after treatment
Immunisation and Vaccination Records	10 years
Joint Replacement Records	10 years

Learning Disabilities (Adult)	20 years, or 8 years if died in care
Learning Disabilities (Child)	25th birthday
Maternity, Midwifery and Neonatal	25 years after birth of last child
Mentally Disordered Persons (Adult)	20 years, or 8 years if died in care
Mentally Disordered Persons (Child)	20 years or 25th birthday if longer
Neonatal Screening Records	25 years
Nicotine Replacement Therapy (Stop Smoking)	2 years
Occupational Health Records (Staff)	3 years after employment termination
Occupational Related Diseases (e.g. Asbestosis)	10 years
Occupational Therapy	8 years adult, 25th birthday child
Oncology, Radiotherapy	30 years
Operating Theatre Lists	4 years
Operating Theatre Registers	8 years
Orthoptic Records	8 years adult, 25th birthday child
Outpatient Lists	2 years after current year
Parent-Held Records	Retrieve, then retain as per record type
Patient-Held Records	Retrieve, then retain as per record type
Physiotherapy Records	8 years adult, 25th birthday child
Podiatry Records	8 years adult, 25th birthday child
Prescriptions	2 years
Psychotherapy Records	20 years, or 8 years if died in care
Litigation Records	As advised by Legal Dept
Records of Destruction of Health Records	Permanently
Recovery Room Records	8 years
Referral Letters	8 years adult, 25th birthday child
Scanned Records	As per record type
Speech and Language Therapy	8 years adult, 25th birthday child

X-Ray Films	8 years adult, 25th birthday child

Appendix F: Corporate Record Retention Periods

Type of Record (Corporate)	**Retention Period**
Accident Records	10 years
Agendas (Board Meetings and Major Committees)	30 years
Agendas (Other)	2 years
Audit Records (Internal and External)	2 years from completion of audit
Business and Local Delivery Plans	20 years
CCTV Images	31 days
Commissioning Decisions and Appeals	6 years
Complaints Documentation	8 years
Data Protection Act Requests	3 years
Freedom of Information Act Requests	3 years, 10 years if withheld
Health & Safety Documentation	3 years
Incident Forms	10 years
Litigation	10 years or as advised by Legal Dept
Meeting & Minute Papers (Major Committees incl. Board)	30 years
Meeting & Minute Papers (Other Committees)	2 years
Mortgage Documents (Acquisition, Transfer, Disposal)	6 years after repayment
PALS Records	10 years
Papers of Minor or Brief Importance Not Covered Elsewhere	2 years
Patient Surveys	2 years
Project Files	6 years
Public Consultations	5 years
Quality & Outcomes Framework (QOF) Documents	2 years
Reports	30 years
Requisitions	18 months

Research Ethics Committee Records	3 years from date of decision
Serious Incident / Serious Untoward Incident (SUI) Files	30 years
Statistics	3 years
Timesheets	2 years
Building & Engineering Works	30 years
Building Plans, Deeds, Drawings & Records	Lifetime of building
Inspection Reports	Lifetime of Installation
Maintenance Contracts	6 years from end of contract
Manuals	Lifetime of equipment
Medical Device Alerts	Until updated or withdrawn
Accounts – Annual (Final)	30 years
Accounts – Receipts, Slips, Counterfoils, Vouchers etc.	2 years
BACS Records	6 years after current year
Contracts	15 years
Creditor Records	3 years after current year
Debtor Records	6 years after current year
Documents Not Mentioned Elsewhere	6 years
Expense Claims	5 years after current year
Fraud Case Files	6 years after current year
General Medical Services Payments	6 years after current year
Invoices, Ledgers, Journals, VAT Records, Bills	6 years after current year
PAYE Records	6 years after employment termination
Payroll	6 years after current year
HR Records (Main Record)	6 years after individual leaves
HR Records (Summary of Record)	Until individuals 70th Birthday
IM&T Software Licenses	Lifetime of software
Job Applications (Successful)	3 years after employment termination

Job Applications (Unsuccessful)	1 year
Leaver’s Dossiers	6 years after employment termination
Personnel / HR Records	6 years after employment termination
Study Leave Applications	5 years
Timesheets	2 years after current year
Tenders (successful)	Tender period plus 6 years
Tenders (unsuccessful)	6 years

Appendix G: Legal Acts Pertaining to this Document

The Data Protection Act 1998: all staff must abide by the Data Protection Act 1998. Personal information relating to staff, suppliers and so on may only be accessed and used by staff on a need to know basis. Unauthorised disclosure of such “personal data” may result in disciplinary action and prosecution. Under the Act personal data must be:

- Obtained and processed fairly and lawfully;
- Processed for limited purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept no longer than necessary;
- Processed in line with the rights of the data subject;
- Appropriate security
- Adequate protection when transferring outside the EEA

Every individual, including staff, is entitled to be informed of any personal data held on them by the organisation, to access that data and to have it corrected if it is inaccurate. gAll enquiries relating to the Data Protection Act must be referred to the Data Protection Officer.

- **The Public Records Act 1956 and 1967 and Freedom of Information Act 2000:** These Acts regulate the storage and publication of records held by public bodies.

- **The Copyright, Designs and Patents Act 1988**: It is illegal to copy, without the appropriate consent, software except for backup purposes, and each machine must have a license for its software. The copyright owner has the right to bring civil proceedings and in certain circumstances criminal proceedings against those that infringe their rights.

- **Department of Health Guidance:** Guidance and standards for the Protection and Use of Patient Information and Caldicott Guardian guidance can be found on the Department of Health website.