Confidentiality and Data Protection Policy and Procedures

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Operating Officer / SIRO
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager / Governance and Board Secretary
Date Approved:	17th January 2019
Committee:	Integrated Governance Committee
Version:	4.0
Review Date:	April 2020

Version History

Version no.	Date	Author	Status	Circulation
1.0	December 2014	IG Associate / Governance & Board Secretary	Presented for approval. Review date set at two years.	Integrated Governance Committee
2.0	December 2016	Senior IG Officer	Approved	Added to Skyline
2.1	May 2017	Governance & Board Secretary	IGC approved amendments to reflect new role of Associate Director of Corporate Affairs	Added to Skyline
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	March 2018	Information Governance Manager	Draft	Review of policy and associated procedures. Amendments to reflect changes under the GDPR (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017).

2.4	April 2018	Information Governance Manager	Draft	Policy approved by IGC subject to minor 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	21st December 2018	Information Governance Manager	Draft	Amended to comply with new Data Security and Protection Toolkit requirements
4.0	17th January 2019	Information Governance Manager	Approved	Approved by IGC January 2019

Contents

Appendices

Glossary of Terms

'Consent' The consent of the 'data subject' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

'Corporate Information' All categories of corporate information should be regarded as confidential in the first instance although they may be releasable through the Freedom of Information Act regime, including via the Publication Scheme. This includes (but is not limited to):

- Board and meeting papers and minutes
- Tendering and contracting information
- Financial information
- Project and planning information

'Data Breach' Data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

'Data Controller' Data Controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

'Data Processor' Processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

'Data Subject' An identified or identifiable natural person.

'Personal Data' Personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier**,** including (but not limited to);

- Name
- Date of Birth
- Post Code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or Hospital/Practice Number
- Location data or online identifier

	Personal data that has been pseudonymised e.g. key coded, can fall within the scope of data protection legislation depending on how difficult it is to attribute the pseudonym to a particular individual.
'Processing'	Processing means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
'Special Category Data'	Special Category Data (or sensitive personal data) are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

1 INTRODUCTION

1.1 NHS Wakefield Clinical Commissioning Group (CCG) is committed to the principles of both accountability and transparency which are enshrined within the General Data Protection Regulation (EU) 2016/679 and Data Protection Act, in relation to its data processing activities.

1.2 The CCG recognises the importance of reliable information, both in terms of the clinical management of individual patients and 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 processes, stores, shares and disposes of information.

1.3 All staff working employed by or providing services to the CCG are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the General Data Protection Regulation (EU) 2016/679 and Data Protection Act and for health and other professionals, through their own professions' Codes of Conduct.

1.4 The CCG places great emphasis on the need for the strictest confidentiality and information security in respect of personal data and special category data (sensitive personal data). This applies to manual and computer records and conversations about service users' treatments. Everyone working for the CCG is under a legal duty to keep service users' information, held in whatever form, confidential and secure. Service users who feel that confidence has been breached may issue a complaint under the CCG complaints procedure or they could take legal action.

2. AIMS AND OBJECTIVES

2.1 The aim of this policy is to ensure that all staff understand their obligations with regard to any information 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.

2.2 The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the General Data Protection Regulation (EU) 2016/679, Data Protection Act and other related legislation and guidance and to support the assertions of the NHS Digital Data Security and Protection Toolkit.

2.3 This policy supports the CCG in its role as a commissioner of health services and will assist in the secure and confidential sharing of personal information (personal data and special category data) with its partner agencies.

3 SCOPE OF THE POLICY

3.1 This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, representatives acting on behalf of NHS Wakefield CCG including the Governing Body and any external organisations acting on behalf of the CCG, including other CCG's in line with contract of employment or contract for services clauses.

This policy covers:

all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of, the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones, smartphones and cameras.

the processing of all types of information, including (but not limited to):

- Transmission of information – verbal, fax, e-mail, post, text and telephone
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

3.2 Confidentiality and data protection within member practices premises is the responsibility of the owner/partners. However, the CCG is committed to supporting member practices in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

3.3 The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and will continue to work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

3.4 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.

4. ACCOUNTABILITY

4.1 Governing Body

The Governing Body is responsible for ensuring that the necessary support and resources are available for the effective implementation of this Policy.

4.2 Integrated Governance Committee

The Integrated Governance Committee is responsible for the review and approval of this policy, related work plans and procedures and will receive regular updates on compliance and any related issues or risks.

4.3 Accountable Officer

The Chief Officer is the Accountable Officer of the CCG and has overall accountability and responsibility for confidentiality and data protection compliance. 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 confidentiality and data protection, are effectively managed and mitigated.

4.4 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of information risk including those relating to confidentiality and data protection compliance. 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.

4.5 Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information. The Caldicott Guardian also has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. A detailed description of the Caldicott Function is given in the Information Governance Policy and Framework.

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.

4.6 Data Protection Officer

The Data Protection Officer (DPO) is responsible for the provision of advice on data protection compliance obligations, data protection impact assessment and monitoring of data protection compliance which includes conducting assurance audits.

The DPO, with the support of the Information Governance Team, is responsible for investigating and reviewing incidents in respect of possible breaches of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act and agreeing recommended actions. The DPO will advise the CCG on the reporting of Serious Incidents Requiring Investigation, and will liaise with the Information Commissioners Office (ICO) in relation to incidents reported to the ICO.

The DPO will be the first point of contact for the ICO on all data protection matters and for individuals whose data is processed by the CCG (employees, service users and the general public).

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.

4.7 Information Governance Lead

The senior level Information Governance (IG) lead for the CCG is the Governance and Board Secretary. The IG Lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance and for liaising with the Information Governance Team in relation to advice and support.

4.8 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 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 (**Appendix 2**) when appropriate.

Information Asset Administrators (IAAs) have delegated responsibility for the operational use of the CCGs information assets.

4.9 Heads of Service

Heads of Service are responsible for ensuring that they and their staff are adequately trained, and are familiar with the content of this policy and its associated procedures and that staff comply with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act, Caldicott Principles, Human Rights Act 1998 – article 8, and the Common Law Duty of Confidentiality. They must ensure that any breaches of the policy are reported, investigated and acted upon.

The lead for Human Resources is responsible for ensuring that the employment contracts of all staff (permanent and temporary) are compliant with the requirements of this policy and that the importance of patient, staff and corporate confidentiality is included in all corporate induction of staff.

4.10 Employees

Confidentiality is an obligation for all staff. Staff should note that there is a Non-Disclosure of Confidential Information clause in their contract of employment and that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on confidentiality issues. Any breach of confidentiality, inappropriate use of health, business or staff records or inappropriate use of a computer system is a disciplinary offence, which could result in dismissal or termination of employment. All breaches of confidentiality must be reported through the Datix incident reporting system, be notified to the SIRO and (in the case of health or social care records) to the Caldicott Guardian.

All employees are personally responsible for compliance with the law in relation to data protection and confidentiality.

4.11 Information Governance Team

NHS Wakefield CCG receives Information Governance support including advice on data protection and confidentiality from the Information Governance Team (which is shared with NHS Calderdale CCG, NHS Greater Huddersfield CCG and NHS North Kirklees CCG).

5. CONFIDENTIALITY CODES OF PRACTICE, GUIDANCE AND LEGISLATION

Information will be defined and where appropriate kept confidential, underpinning the principles of Data Protection legislation, Common Law, Caldicott, NHS Digital Guidance and professional Codes of Practice and associated legislation.

5.1 General Data Protection Regulation (EU) 2016/679 and Data Protection Act - Data Protection Principles

All information and data which can identify a natural person, held in any format (visual/ verbal / paper / electronic / digital media etc.) is safeguarded by data protection legislation. The legislation includes six principles which set out the main responsibilities for the CCG in relation to data protection law.

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

5.3 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except as originally understood or with subsequent consent.

In some instances, judgements have been given which recognise a public interest in disclosure but these are on a case by case basis. United Kingdom courts rely extensively on this duty of confidentiality coupled with the Human Rights Act 1998 in making decisions on breaches of confidence.

The Duty of Confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

5.4 Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS structure. Dame Fiona was asked to conduct a further review and a new report: 'Information: to share or not to share' was published in March 2013. The recommendations of this report have been largely accepted by the government and a further Caldicott Principle (principle 7) is now included alongside the existing six principles:

Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.

Don't use personal confidential data unless it is absolutely necessary
Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Understand and comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

The duty to share information can be as important as the duty to protect patient confidentiality
Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by

these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5.5 NHS Digital Guidance

The Health and Social Care Information Centre (now NHS Digital) was established in April 2013 and is responsible for facilitating the management and sharing of data across the re-configured NHS to support both operational and other functions such as planning, research and assessments. NHS Digital produced a Code of Practice: 'A Guide to Confidentiality in Health and Social Care' in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

5.6 The NHS Care Record Guarantee and Social Care Record Guarantee for England

The NHS Care Record Guarantee and Social Care Record Guarantee for England set out the rules that govern how individual care information is used in the NHS and Social Care. They also set out what control the individual can have over this.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

5.7 Health and Social Care (Safety and Quality) Act 2015

The 2012 Act introduced changes regarding access to patient confidential data and placed particular restrictions on access to patient data by commissioning organisations and their support organisations. The 2015 Act introduced provision about the safety of health and social care services in England, about the integration of information relating to users of health and social care services in England and about the sharing of information relating to an individual for the purposes of providing that individual with health or social care services in England. In particular it introduced a duty to share the NHS number for direct care purposes.

5.8 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable. Regulations under the Act support the sharing and use of information for defined commissioning activities and support NHS structure subject to safeguards.

5.9 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access to data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

5.10 Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which govern the sharing of very specific types of data in such areas as;

- Safeguarding Children
- Sexually Transmitted Diseases
- Terminations, Assisted Conception
- Registration of Births and Deaths
- Criminal Investigations
- Terrorism
- Communicable Diseases

This is not an exhaustive list and further guidance can be obtained from the organisation's Caldicott Guardian, Senior Information Risk Owner (SIRO) or the Information Governance Team.

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

All staff are bound by the codes of conduct produced by their professional regulatory body (where relevant), by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice for Health and Social Care sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

6 PROCEDURE

6.1 General principles

- The CCG is committed to the principles of accountability and transparency in its processing of personal data and special category data under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act.
- The CCG will maintain records on its data processing activities and will conduct regular reviews of the personal data processed and update records of data processing activities accordingly.
- The CCG regards all identifiable personal information (personal data and special category data) relating to service users, staff and others coming into contact with the CCG as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The CCG regards all identifiable personal information (personal data and special category data) relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The CCG will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act, Human Rights Act, the common law duty of confidentiality, the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable confidentiality and data protection controls are in place.

6.2 Codes of Conduct and Certification Mechanisms

The CCG will aim to work towards and adhere to any relevant Codes of Conduct and certifications that cover the CCGs data processing activities in order to demonstrate compliance with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (Articles 40 and 42).

6.3 Data Protection Fee

Under the Data Protection (Charges and Information) Regulations 2018 and as an organisation that determines the purposes for processing personal data, the CCG will pay an annual fee to the Information Commissioners Office. The DPO will ensure the annual fee is paid by the date due.

6.4 Individuals Rights

The CCG acknowledges the rights individuals have in respect to their personal information (personal data and special category data) processed by the CCG and will take steps to ensure these are managed in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act.

6.4.1 The Right to be Informed

The CCG will ensure privacy notices are intelligible and easily accessible and meet the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act. The CCG will make Privacy Notices available at the time of collection of the personal data and where personal data is obtained through other sources, the CCG will provide individuals with privacy information within a reasonable period of time and no later than one month.

Where relevant the CCG will ensure privacy notices are written in a language children will understand.

The CCG will maintain a comprehensive privacy notice on its public website.

Please contact the CCG IG Team for advice on the process to follow for providing information about processing and individuals' rights at the correct time.

6.4.2 The Right of Access

Individuals have a right of access to information held about them by the CCG in line with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act.

The procedure for the management of the right of access is set out in the Subject Access Request and Access to Health Record Procedure (within the Records Management and Information Lifecycle Policy and Procedure). This procedure also gives guidance in relation to requests for the records of deceased individuals under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

All staff should familiarise themselves with the Subject Access Request and Access to Health Record Procedure which should be followed for all requests for personal data.

Access to corporate information and records will be in accordance with CCG's Freedom of Information Act and Environmental Information Regulations Policy.

6.4.3 The Right to Rectification

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act provides individuals with the right to have their personal data rectified if it is inaccurate or incomplete.

A request under the right to rectification may sometimes follow a subject access request.

The outline process for managing requests for personal date to be rectified is set out in **Appendix 5**.

6.4.4 The Right to Erasure

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act provides individuals with the right to erasure which is also known as the 'right to be forgotten'. The right to erasure is not an absolute 'right to be forgotten'. In law individuals only have a right to have personal data erased and to prevent processing in specific circumstances. Individuals have the right if:

- the personal data is no longer necessary for the purpose which the CCG originally collected or processed it for;
- the CCG is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- the CCG are relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the CCG are processing the personal data for direct marketing purposes and the individual objects to that processing;
- the CCG have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- the CCG have to do it to comply with a legal obligation; or
- the CCG have processed the personal data to offer information society services to a child.

The CCG may refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

- for the establishment, exercise or defence of legal claims.

There are two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services).

The outline process for managing requests for personal date to be erased is set out in **Appendix 5**.

6.4.5 The Right to Restrict Processing

The General Data Protection Regulation (EU) 2016/679 and Data Protection Act provides individuals with a right to 'block' or suppress processing of their personal data. In law there are some specific circumstances where the CCG is required to restrict the processing of personal data, some of which relate other 'rights' exercised by the individual. The right applies in the following circumstances:

- the individual contests the accuracy of their personal data and you are verifying the accuracy of the data;
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- you no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data under Article 2 and you are considering whether your legitimate grounds override those of the individual.

The outline process for managing requests for personal date to be erased is set out in **Appendix 5**.

6.4.6 The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The CCG will provide the personal data in a structured, commonly used and machine readable format and provide the information free of charge.

The outline process for managing requests for data portability is set out in **Appendix 5**.

6.4.7 The Right to Object

Individuals have the right to object to the processing of their personal data when it is processed on the grounds of 'legitimate interests' or the 'performance of a task' in the public interest/exercise of official authority (including profiling), when it is processed for direct marketing or processed for the purposes of scientific/historical research and statistics. There are particular conditions attached to each of the above.

In relation to the above grounds for processing and purposes of use, the CCG will inform individuals of their right to object 'at the point of first communication' and in privacy notices.

The outline process for managing requests under the right to object is set out in **Appendix 5**.

The NHS has introduced a new data opt-out provision. This allows people to opt out of their confidential patient information being used for research and planning. If a patient wants to change their choice, they should use the new national data opt-out service to do this. You can find out more about the service at the web address here: https://www.nhs.uk/your-nhs-data-matters/

6.4.8 Rights in Relation to Automated Decision Making and Profiling

In the event that the CCG carries out any processing deemed to involve automated decision making about an individual (making a decision solely by automated means without any human involvement) or undertakes any profiling activity (automated processing of personal data to evaluate certain things about an individual), it will take steps to ensure the individual's right is managed in accordance with the requirements of the General Data Protection Regulation (EU) 2016/679 and Data Protection Act.

6.5 Consent

The CCG will establish, record and inform individuals about the lawful basis that it is relying on to process personal data.

Consent is one way that the CCG may comply with data protection law, but it is not the only way and it will take due regard to other lawful bases available to it, to process personal data. Where the CCG identifies a basis other than consent to process personal data, it will still consider what actions need to be taken to satisfy the Common Law Duty of Confidentiality. One action may be the use of a consent based processes to ensure that the Common Law Duty of Confidentiality is properly satisfied and that there are no surprises for individuals in the use of their personal data by the CCG.

6.6 Using and Disclosing Confidential Patient Information for Direct Healthcare

For common law purposes consent to share personal information for direct care is usually on the basis of implied consent, which may also cover administrative purposes where the individual has been informed or it is otherwise within their reasonable expectations. When information sharing is needed for direct healthcare patients should still be informed about;

- The use and disclosure of their healthcare information and records
- The choices that they have and the implications of choosing to limit how information may be used or shared
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations
- The potential use of their records for the clinical governance and audit of the care they have received.

Under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act for processing of personal data in the delivery of direct care and for administrative purposes, the following conditions of lawful processing that are available to all publically funded health and social care organisations in the delivery of their functions will apply:

- GDPR Article 6 (1) (e) 'for the performance of a task carried out in the public interest or in the exercise of official authority, and

- GDPR Article 9 (2) (h) 'medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems'.

6.7 Using and Disclosing Confidential Staff Information

Consent to disclose can usually be taken to be implied when the information sharing is needed for direct communications related to their role, salary payment and pension arrangements. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of Freedom of Information Request where the Public Interest in Disclosure is deemed to override confidentiality considerations.

6.8 Sharing Confidential Personal Information without Consent

It may sometimes be necessary to share confidential personal information without consent. On occasion it may be necessary to disclose personal information when this is against the known wishes of the individual or where the individual has expressly refused to consent. There must be a legal basis and strong justification for sharing personal information in such circumstances or a court order (ordering the disclosure) must be in place;

- Discuss the request with the Caldicott Guardian and/or the DPO.
- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- If the request is from the police or another enforcement agency ask for the appropriate request form in line with the Subject Access Requests and Access to Health Records Procedure. This should clearly evidence the legal power or duty under which the police are making the request.
- Follow any locally agreed Information Sharing Protocols and national guidance.
- Information may also be shared with Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.
- Consider the 7th Caldicott Principle in the context of the request **The duty to share information can be as important as the duty to protect patient confidentiality.**

6.9 Personal Data Relating to Children

Where processing is likely to involve children's personal data, the CCG will ensure relevant privacy notices are written so that they are able to understand what will happen to their personal data and the rights they have.

The CCG will undertake Data Protection Impact Assessments where data processing is likely to involve the processing of children's data and is likely to result in a high risk to the rights and freedoms of children.

6.10 Data Protection by Design and Default

It is a requirement of the General Data Protection Regulation[1] and Data Protection Act that organisations put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual's rights. This is known as 'data protection by design and by default'.

[1] General Data Protection Regulation[1] (EU) 2016/679

Without limitation, all new projects, processes and systems (including software and hardware) must meet data protection by design and meet confidentiality requirements. To enable the organisation to identify and minimise any data protection risks a Data Protection Impact Assessment (DPIA) must be undertaken when processing of personal data is likely to result in a 'high risk to individuals'. A DPIA will:

- Identify privacy risks to individuals and fix problems at an early stage
- Demonstrate compliance with the CCGs data protection obligations
- Meet individuals expectations of privacy
- Help avoid reputational damage which might otherwise occur

All staff should ensure they are familiar with the contents of this procedure.

6.11 Anonymisation and Managing Data Protection Risk

Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data. Anonymisation is of particular relevance, given the increased amount of information being made publicly available through the Governments Open Data agenda. The Protection of Freedoms Act 2012 enhances access to information by requiring a public authority to consider data held in a dataset that is not already published. Where the Freedom of Information Act 2000 requires the publication of a dataset the CCG is required to release it in a form that is reusable.

The CCG will ensure that data released under the Freedom of Information Act 2000 and governments Open Data Agenda are fully anonymised. All staff will adhere to the Information Commissioners 'Anonymisation Code of Practice' which describes the steps an organisation must take to ensure that anonymisation is conducted effectively, while retaining useful data.

6.12 Protecting Information

Staff must follow good practice principles and comply with appropriate legislation when working with confidential information:

- Discussions on confidential matters should take place where they cannot be overheard. Take care in public places and at social events.
- Confidential information should never be left open and unattended on a desk.
- Confidential information not in use should be locked away securely.
- Storage systems should be secure and be kept locked at all times.
- All information assets held should be recorded on the Information Asset Register.
- Access to confidential information should be limited to the minimum necessary.
- Consent to share confidential information should be recorded and the sharing limited to that which was agreed.

- Use sealed envelopes marked confidential when sharing confidential information with internal colleagues.
- Confidential paper records must not be taken outside of the workplace except in line with an agreed protocol or procedure.
- Comply with the organisation's procedures for disposal of confidential electronic or paper information.
- Comply with the organisation's policies and procedures on all aspects of
- information security and seek advice if you are unsure.
- Work related information or images should not be uploaded to social media sites.
- Confidential information must not be given out over the phone except in line with an agreed protocol or procedure.

Additional guidance when working with electronic equipment:

- Ensure you have read and understood the organisation's information security
- Policies and procedures.
- Computer screens should be locked whenever you are away from your device
- Log off when you have finished using a computer.
- Always remove a Smartcard when you are away from your desk even for a few minutes.
- Restrict access to confidential information which is stored on the server.
- All portable media equipment must be encrypted including memory sticks.
- Downloading confidential information to a non NHS portable device is forbidden.
- Retain confidential information in line with business requirements and record retention schedules.
- Seek advice on fully deleting computer data if you are unsure.
- Follow password guidance and change passwords regularly.
- NEVER share a password or Smartcard with anyone or accept an instruction to do so.
- Electronic equipment must only be disposed of via The Health Informatics Service.
- Portable devices must not be left unattended and on display e.g. in the foot well of a car or passenger seat.
- Keep back-up tapes, memory sticks etc. separate to your mobile device
- Password protect mobile devices with a strong password.
- Mobile storage devices must only be used in line with agreed local procedures.
- Information should only be kept on encrypted mobile devices for short term operational reasons and this should be backed up to a server regularly.

All staff are personally responsible for ensuring the safe processing of information.

6.13 Transferring Information

All paper transfers of confidential information must be secure:

- If your department needs to routinely transfer confidential information internally or externally ensure that there is an agreed protocol for such transfers.
- Only use sealed envelopes for confidential information.
- Fully address envelopes and mark them private and confidential regardless of
- How they are to be transferred.
- Large or particularly sensitive files should be double enveloped and sent recorded delivery, hand delivered or a courier should be used.
- Follow up transfers of sensitive confidential information to check receipt.
- Keep confidential information being transported by car out of sight. Ensure it is not left unattended or in the car overnight.
- Special consideration is needed for transfer of information outside the European Economic Area. Please contact the Information Governance Team for further advice.

All electronic transfers of confidential information must be secure:

- Follow all Information Security policies and procedures including the guidance within the IG User Handbook.
- Seek advice from the Information Governance Team or the DPO, if you have any concerns as to the disclosure and/or security of transfer arrangements.
- Emails - users must follow the E-Communications and Social Media Policy and Procedure and best practice guidance on transmitting confidential information.
- Only use approved NHS e mail accounts. Confidential patient and staff information may only be transferred using NHS Mail or an approved method of encryption.
- Ensure you do not send confidential information to a personal e mail address. If a member of the public makes a request to correspond by email e.g. complaints or individual funding request correspondence, using their non-secure email address, it is the responsibility of the member of staff to ensure the member of public is provided with a clear explanation of the risks of using unsecure email addresses and consent must be obtained.
- Do not forward emails containing offensive information. Contact the Service Desk (THIS) for advice.
- Where there is a business requirement to download or transfer confidential data, seek advice from the Information Governance Team in the first instance who will advise if the approval of the DPO is required.
- Confidential information should only be transmitted by fax where there is no secure alternative method of transfer available. A cover sheet should be used at all times giving names and contact details of both sender and recipient.
- Check fax numbers regularly, programme them in where possible, send a test fax before sending confidential information and ring to check receipt of all faxes sent.
- Ensure the fax will be received in a safe haven or that a named individual is there to collect it immediately.
- Ensure confidential correspondence is not left unattended on the fax machine if there is a delay in transmission.

6.14 Records Management

The CCG has a Records Management and Information Lifecycle Policy which should be followed for all aspects of record creation, sharing, storage, retention and destruction of records.

6.15 Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and it should only be disclosed, when appropriate, through the proper processes.

6.16 Information Sharing

The organisation will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Data Sharing Code of Practice and the additional safeguards introduced by the Health and Social Care Act 2012.

The CCG is a signatory to the Information Sharing Protocols which should be followed at all times.

Where appropriate the CCG will ensure it is proactive in putting specific information sharing agreements in place to support information governance and transparency requirements.

6.17 Using NHS Numbers

The NHS Number is the national, unique identifier that makes it possible to share patient and service user information across the NHS and social care safely, efficiently and accurately. The Health and Social Care (Safety and Quality) Act 2015 which places a legal obligation on organisations that commission or provide health care or adult social care to include a consistent identifier when processing patient and service user information for purposes that might facilitate the provision of health services and adult social care to individuals.

The CCG will ensure the NHS Number is used as consistent identifier for direct care purposes and that staff follow the NHS Number Principles of Find It, Use It and Share It.

Staff involved with recording service user data need to ensure that it is performed in a timely manner and that the details being recorded are checked with the source at every opportunity. In situations where data is shared between systems it is imperative that the source data be validated initially.

Staff must ensure all patient and service user identifiers including the NHS number are appropriately used and kept secure and confidential. Information sharing agreements or contracts should ensure that the confidentiality and

security standards are clear and complied with. The Common Law Duty of Confidentiality and Data Protection legislation constraints continue to apply. If there is a legal basis for sharing information (e.g. consent) and the purpose is likely to facilitate care, then the information must be shared and where it would not require unreasonable effort the NHS Number must be included.

6.18 Confidentiality Audit Procedures

In order to provide assurance that access to confidential person identifiable information is gained only by those individuals that have a legitimate right of access to the information, the CCG ensures that access to person identifiable information is monitored on a regular basis.

Confidentiality audits focus not just on controls within electronic information management systems, but also on physical access to paper based information. Audits may identify whether confidentiality has been breached, or put at risk through deliberate misuse of a system, or as a result of weak, non-existent or poorly applied controls.

Regular audits will be carried out in line with the Confidentiality Audit Procedures in **Appendix 3**.

6.19 Personal Data Breaches

All staff need to be aware of their responsibilities for keeping personal information physically secure and ensuring the confidentiality of such information held by the CCG. The duty of confidentiality is written into employment contracts.

A breach of confidentiality of information gained, whether directly or indirectly, in the course of duty may be a disciplinary offence which could result in dismissal and/or prosecution. No employee shall knowingly misuse any information or allow others to do so. It is a disciplinary offence to access records/ information that you have no legitimate reason to view this includes, records about yourself, your family, friends, neighbours, acquaintances. If you do not have a legitimate reason to access, do not browse. Remember all transactions are auditable.

All actual, potential or suspected personal data breaches including breaches of confidentiality must be reported via the CCG's Incident Reporting Policy. All incidents involving patient data should additionally be reported to the Caldicott Guardian. The DPO should consider whether serious breaches of confidentiality or those involving large numbers of individuals need to be reported to the Information Commissioner via the national process for reporting, managing and investigating information governance serious incidents. It is a legal requirement to report certain types of incident to the Information Commissioners Office. Where this is required, it must be undertaken within 72 hours of becoming aware of the incident, where feasible.

What should be reported through the incident reporting process?

Misuses of personal data and information security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same incident does not occur again. The following list gives some examples of personal data and information security related incidents which should be reported:

- Sharing of passwords.
- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that the disclosure is not in accordance with the Data Protection Act and the Confidentiality: NHS Code of Practice.
- Transferring or transmitting data in a way that breaches confidentiality.
- Leaving confidential information lying around in public area e.g. photocopier.
- Theft or loss of patient-identifiable or staff identifiable information.
- Disposal of confidential information in a way that breaches confidentiality
- i.e. disposing of patient record and or content of, in ordinary waste paper bin.

7 TRAINING & GUIDANCE

7.1 Mandatory Training

All staff will receive annual Data Security Awareness training and guidance through the CCG's Mandatory Training Programme.

Training will be delivered through the Electronic Staff Record e-learning platform managed on behalf of the CCG by NHS Sheffield CCG.

All line managers must actively ensure that their staff undertake and complete the annual mandatory Data Security Awareness training.

7.2 Specialist Training

Additional training may be sourced or provided by the organisation for specialist functions such as the Senior Information Risk Owner role, Caldicott Guardian role, Data Protection Officer role, Subject Access function and Data Protection Impact Assessment.

7.3 Awareness and Compliance

Staff are effectively informed about their responsibilities and this policy through annual Data Security Awareness training and other awareness sessions, the IG User Handbook, briefing notes or a combination of these.

8 IMPLEMENTATION AND DISSEMINATION

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

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

9 MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

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

Compliance with the mandatory assertions of the Data Security and Protection Toolkit. The Integrated Governance 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. The Integrated Governance Committee will monitor progress via the Workforce Report.

Statistically validated reduction in Information Governance related incidents. Monitoring of incidents by the Integrated Governance Committee.

No Data Protection enforcement activity undertaken utilising the 'investigatory powers' or 'corrective powers' of the Information Commissioner. Corrective powers include: reprimands, bans on processing, suspension of data transfers, ordering the correction of an infringement and administrative fines.

No Freedom of Information Act enforcement notices served on the organisation. The Integrated Governance Committee will monitor progress via the Information Governance Update Report.

Staff know who and where to direct data protection and confidentiality concerns and queries to. Results of annual information governance staff survey.

10 REFERENCES

- General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017)
- Freedom of Information Act 2000
- Human Rights Act 1998
- Common Law Duty of Confidence
- Health and Social Care Act 2012
- NHS Act 2006

- Health and Social Care (Safety and Quality) Act 2015

11 ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

The CCG has a suite of information governance and supporting policies including:

- Information Governance Policy and Framework
- Information Security Policy (Incorporating Network Security)
- Record Management and Information Lifecycle Policy and Procedures
- Incident Reporting Policy
- Integrated Risk Management Framework
- Freedom of Information Act and Environmental Information Regulations Policy
- System Level Security Procedures
- Electronic Communications and Social Media Policy and Procedure

And their associated procedures (including but not limited to)

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

This policy should be read in conjunction with the Information Governance User Handbook which has been shared with all staff and for which new staff will need to sign for receipt and confirm that they have read the document.

12 EQUALITY IMPACT ASSESSMENT

Attached at **Appendix 1** Equality Impact Assessment.

Appendix 1

Equality Impact Assessment

Title of policy	Confidentiality and Data Protection Policy and Procedures
Names and roles of people completing the assessment	Governance and Board Secretary and Information Governance Manager
Date assessment started/completed	March 2018

1. Outline	
Give a brief summary of the policy	The aim of this policy and procedure is to ensure that all staff understand confidentiality and data protection obligations with regard to personal and confidential information which they come into contact with in the course of their work. The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the General Data Protection Regulation (EU) 2016/679, Data Protection Act and associated legislation and guidance.
What outcomes do you want to achieve	That the CCG has compliance with the requirements of General Data Protection Regulation (EU) 2016/679, Data Protection Act and other related legislation and guidance. That all staff understand confidentiality and data protection obligations with regard to personal confidential information which they come into contact with in the course of their work. That no Data Protection enforcement activity is undertaken utilising the 'investigatory powers' or 'corrective powers' of the Information Commissioner.

2. Analysis of impact

This is the core of the assessment, using the information above detail the actual or likely impact on protected groups, with consideration of the general duty to: eliminate unlawful discrimination; advance equality of opportunity; foster good relations			
	Are there any likely impacts? Are any groups going to be affected differently? Please describe.	**Are these negative, positive or neutral?**	**What action will be taken to address any negative impacts or enhance positive ones?**
Age	No	Neutral	
Disability	The new data protection framework protects personal data 'concerning health' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). Additional safeguards are provided throughout the new data protection framework.	Neutral	The overall effect is that the grounds for processing sensitive personal data are broadly comparable to the Data Protection Act 1998.
	The standards of consent are higher under the new data protection framework than under the 1998 Act. This may have an impact on those incapable of giving consent which is 'freely given, specific, informed and unambiguous', such as those who have a learning disability.	Positive	Under the GDPR, consent to process personal data can be given legally by another with a lasting power of attorney or through the Court of Protection.
Gender reassignment	No	Neutral	
Marriage and civil	No	Neutral	

partnership			
Pregnancy and maternity	The new data protection framework protects personal data 'concerning health' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). Additional safeguards are provided throughout the new data protection framework.	Neutral	The overall effect is that the grounds for processing sensitive personal data are broadly comparable to the Data Protection Act 1998.
Race	The new data protection framework protects personal data 'revealing racial or ethnic origin' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4).	Neutral	The overall effect is that the grounds for processing sensitive personal data are broadly comparable to the Data Protection Act 1998.
Religion or belief	The new data protection framework protects personal data regarding 'religious or philosophical beliefs' as a 'special category of data' (in the case of Part 2) and processing of it as 'sensitive processing' (in the case of Parts 3 and 4).	Neutral	The overall effect is that the grounds for processing sensitive personal data are broadly comparable to the Data Protection Act 1998.
Sex	No	Neutral	
Sexual orientation	The new data protection framework protects personal data 'concerning sex life and sexual orientation' as a 'special category of data' (in the case of Part 2)	Neutral	The overall effect is that the grounds for processing sensitive personal data are broadly comparable to the Data Protection Act

	and processing of it as 'sensitive processing' (in the case of Parts 3 and 4). The existing condition for processing personal data 'for the purpose of identifying or keeping under review the existence or absence of equality of opportunity' is newly expanded to include personal data concerning an individual's sexual orientation.		1998.
Carers	No	Neutral	
Other relevant group	No	Neutral	
Human Rights	No	Neutral	
Health Inequalities	No	Neutral	

3.	
If any negative/positive impacts were identified are they valid, legal and/or justifiable? **Please detail.**	No anticipated detrimental impact on any equality group. The new data protection framework maintains the strong protections that currently exist to protect individuals and the processing of personal data that would reveal protected characteristics. The policy is applicable to all staff and adheres to legal requirements and best practice. There are no statements, conditions or requirements that disadvantage any particular group of people with a protected characteristic.

4. Monitoring, Review and Publication

How will you review/monitor the impact and effectiveness of your actions	Monitoring of any issues of unlawful treatment of protected groups of staff (or others) (such as harassment or discrimination) relating to the implementation of this Confidentiality and Data Protection Policy and Procedures.		
Lead Officer	Governance and Board Secretary	**Review date:**	February 2020

5.Sign off			
Lead Officer	Equality and Diversity Advisor		
Director		**Date approved:**	

Appendix 2

Data Protection Impact Assessment Procedure

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Finance Officer
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager / Governance & Board Secretary
Date Approved:	[enter approval date]
Committee:	Integrated Governance Committee
Version:	4.1
Review Date:	April 2020

Version History

Version	Date	Author	Description	Circulation
1.0	March 2010	Senior Confidentiality IM & T Security Officer	Final	Approved by Information Governance Group
2.0	Jan 2014	Associate Specialist IG	Approved	Policy approved by Integrated Governance Committee on 16 January 2014
3.0	December 2016	Senior Information Governance Officer	Approved	Added to Skyline
3.1	April 2018	Information Governance Manager	Draft	Review of procedure. Amendments to reflect changes under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017).
4.0	April 2018	Information Governance Manager	Approved	Approved by IGC April 2018

4.1	21st December 2018	Information Governance Manager	Draft	Amended to comply with new Data Security and Protection Toolkit requirements

Contents **Page**

1. Introduction

This procedure explains the principles which form the basis for a Data Protection Impact Assessment (DPIA) and sets out the basic steps which all staff must follow during the initiation phase or early assessment of the development and implementation of projects and business changes.

A DPIA should be seen as a separate process from compliance checking or data protection audit processes and is also a requirement of the Data Security and Protection Toolkit which helps the CCG to comply with the data protection by design and default principles within data protection legislation. DPIAs are based on current legal requirements and professional best practice[2].

This procedure reflects the minimum requirements under Article 35 of the GDPR and should be read in conjunction with the Confidentiality and Data Protection Policy and Procedures which is available on the Intranet.

All staff must recognise that a DPIA01 form and declaration must be completed and submitted to the IG Team in the following circumstances and situations:

- Collection, retrieval, obtaining, recording or holding of new personal data or information.

- A change to existing processes, technology or products which will significantly amend the way personal data or information is handled.

- The implementation or development of new processes, technology or products which involve the use of personal data or information.

- The use of a trial period of technology or products which use personal data or information.

- The use of charitable or free technology or products which use personal data or information.

- Publishing personal data or sensitive information on the internet or in other publically available media types.

- Procurement of technology or products which use personal data or information.

- De-commissioning or disposal of technology or products which use personal data or information.

[2] Under the GDPR, full DPIA's must be signed off by the appointed Data Protection Officer.

2. Purpose

The purpose of this procedure is to ensure that risks to the rights and privacy of individuals are minimised while allowing the aims of the project or business change to be met whenever possible.

This procedure provides a standardised approach towards identifying, assessing and mitigating data protection and privacy risk and assists towards the delivery of compliance with legal statutory requirements.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of data, technology and processes will work in practice. This analysis can be tested by consulting with the stakeholders who will be working on, or affected by, the project or business change.

3. Background

Infringing on the freedoms and rights as well as the privacy of individuals can damage reputations, services, organisations and individuals. Because harm can present itself in different ways, demonstrable evidence that consideration has been given to the sources of data protection and privacy risks is a legal requirement.

Privacy Impact Assessments (PIAs) are widely used in the UK, especially by government departments and agencies, local authorities, NHS organisations as well as private organisations.

The GDPR DPIA process is the result of an extensive analysis of existing PIA processes; essentially altering the scale, scope and complexity of the way in which PIA's are conducted.

4. Responsibilities

4.1 Responsible Project Leads and Service Managers

Examine the project or business change at the earliest possible stage and make an initial assessment of data protection and privacy risks, by ensuring a DPIA01 form and declaration is completed and submitted to the IG Team by e-mail.

Accept accountability where some of the screening questions within the DPIA01 form apply to the project or business change; therefore, it is likely that a full DPIA must be undertaken.

Recognise that should a full DPIA be deemed to be necessary, there is a legal obligation at this stage for the Data Protection Officer to be involved and the DPIA outcome must be integrated into any project plan before the project is developed and implemented.

Communicate with the IG Team, Data Protection Officer, IT, relevant Information Asset Owner and other key stakeholders for support and advice as required, managing potential sources of risk and concerns as they arise.

Should a full DPIA be necessary, communicate with Data Protection Officer to work towards finalising any conclusions and recommendations.

Where the conclusions and recommendations have been provided by the Data Protection Officer and are:

Accepted: Demonstrate that consideration has been given to the sources of potential risk through the completion of a DPIA OUTCOME form. Additionally conclusions and recommendations are integrated into the main project plan.

Not Accepted: Demonstrate that consideration has been given to the sources of potential risk through formally providing the rationale of non-acceptance by the completion of a DPIA OUTCOME form. Additionally conclusions and recommendations are integrated into the main project plan.

Co-operate and provide the ICO with evidence of the updated project plan and DPIA, if requested.

4.2 Information Governance Team

Carry out an evaluation of the submitted DPIA01 form and declaration, to address the initial sources of potential risk.

Provide the responsible project lead/Service Manager with guidance and support, if required.

Provide the responsible project lead/Service Manager and Data Protection Officer with any recommendations or conclusions that seem necessary.

Escalate any uncooperative actions such as not accepting the risks, not carrying out mitigating tasks etc. to the Data Protection Officer.

4.3 Data Protection Officer

Carry out an evaluation of the full DPIA to identify potential risks and sources.

Escalate any uncooperative actions to the SIRO.

Provide the responsible project lead/Service Manager and relevant Information Asset Owner with any recommendations and conclusions that seem necessary from the evaluation.

Escalate unaccepted conclusions and recommendations to the SIRO.

Communicate with the relevant stakeholders including the responsible project lead/Service Manager, IG Team, IT, relevant IAO and SIRO as necessary. Liaise with the Information Commissioners Office when necessary.

4.4 Information Asset Owner

It is the responsibility of the IAO to develop and manage the standard operating procedures and data quality processes for the appropriate use of the information defined within the project.

5. Is a DPIA required for every Project/Business Change?

Not every project/business change will require a DPIA. The ICO envisages DPIAs being used only where a project/business change includes the use of personal data, or where there could be a risk to the privacy of the individual. DPIAs will usually be recommended where new and intrusive technology is being used, or where private or sensitive personal information which was originally collected for a limited purpose is going to be reused in a new and unexpected way. The DPIA01 Screening Form will help determine if a DPIA is required and if so which of the two options will be suitable.

6. Publishing DPIA's

All DPIA's will be included within the organisation's Publication Scheme. It is acknowledged that DPIA's may contain commercially sensitive information such as security measures or intended product development. It is acceptable for such items to be redacted but as much of the document should be published as possible given all information within a public organisation can be requested through the Freedom of Information Act 2000 and will be listed in the Publication Scheme.

7. Frequently Asked Questions

What is a DPIA?
Also known as PIA, a DPIA is a tool to help the CCG and staff, identify and reduce or fix any data protection or privacy risks before the project or business change commences.

What is the purpose of a DPIA?
An effective DPIA can reduce the risks or potential harm to individuals through scenarios such as the misuse of sensitive personal information or unlawful disclosure of personal information. It can also help design more

efficient and effective process for the management of personal information as part of the project or business change.

What is the basis for a DPIA?
A DPIA01 screening form and declaration must be undertaken for all projects or business changes which involve the use of personal data, technologies and processes.

This also includes a change that will significantly amend the way in which personal data is handled, regardless of whether a full data protection and privacy assessment was deemed to be necessary.

What are the risks of not conducting a DPIA?
Ultimately there are financial penalties that can be applied by the Information Commissioners Office for failure to process personal information lawfully.

Who should carry out a DPIA?
The DPIA01 screening form and declaration must be completed by any member of staff responsible for accomplishing project and business objectives and outcomes.

When should a DPIA be conducted?
It is important that the DPIA01 screening form and declaration is completed and submitted in the early stage of the project or business change, when the project is being designed; you know what you want to do; you know how you want to do it; and you know who else is involved.

It must be completed before decisions are set in stone; you have procured systems; you have signed contracts/memorandums of understanding / agreements; and while you can still change your mind.

If some of the screening questions within the DPIA01 form apply to the project/business change; it is likely that a full Data Protection and Privacy Impact Assessment must be undertaken.

At this stage the Data Protection Officer must be involved and the outcomes must be integrated into the project plan before the project is developed and implemented.

What is the outcome of a DPIA?
The effective outcome of a DPIA should be the minimisation of data protection related risks and a demonstration that consideration has be given to the sources of potential risk and compliance with data protection law.

8. Related Policies and Procedures

- Information Security Policy (incorporating Network Security)
- Confidentiality and Data Protection Policy and Procedures
- Safe Haven Guidelines and Procedure
- Records Management and Information Lifecycle Policy and Procedures

9. Relevant Statutory Legislation and Law

- General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality

10. Further Reading and Guidance

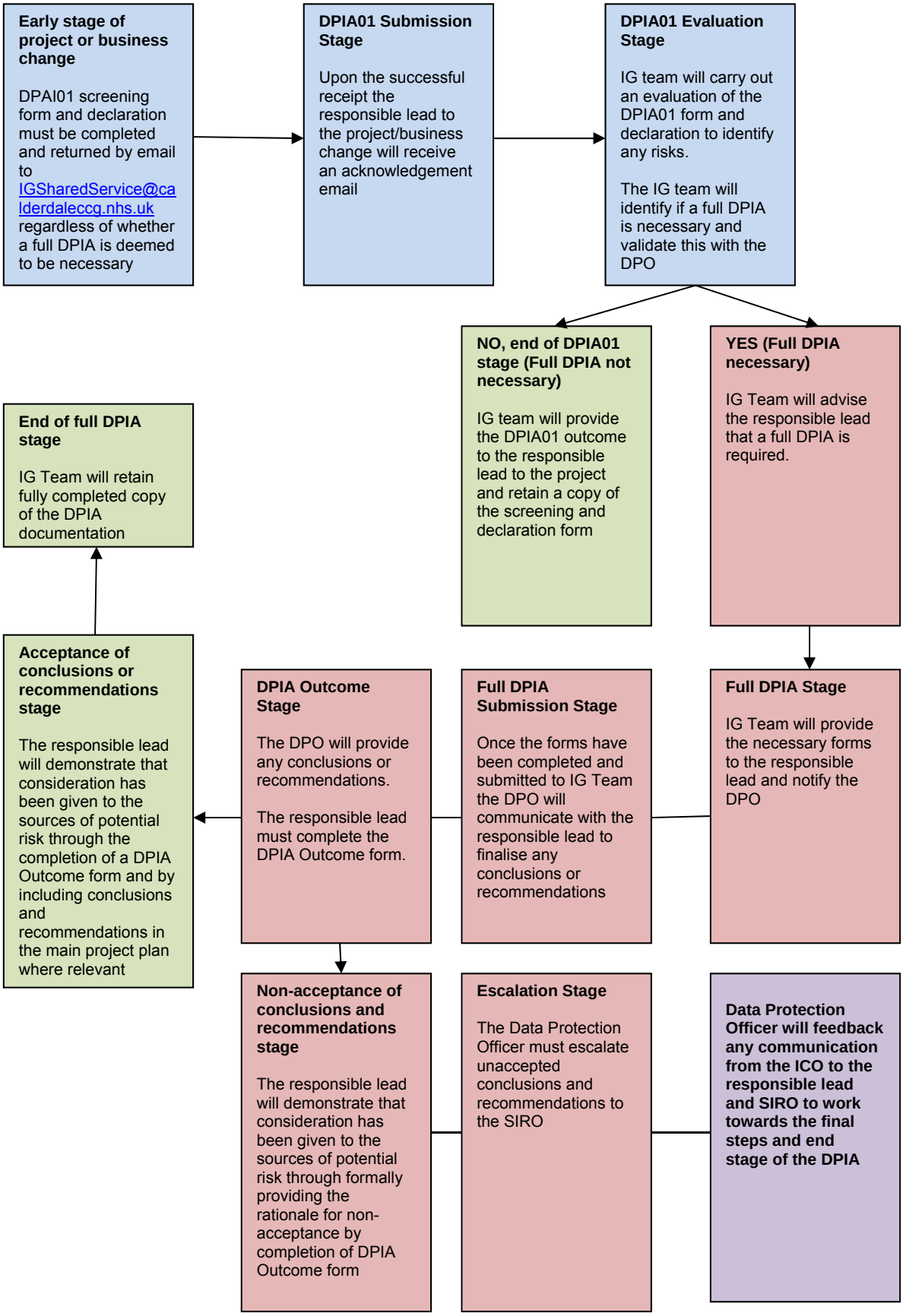
- The ICO's Anonymisation: managing data protection risk code of practice may help identify privacy risks associated with the use of anonymised personal data. It's a short video covering the subject
- The ICO's Privacy Notices: Code of Practice.
- The ICO's Data sharing: code of practice may help to identify privacy risks associated with sharing personal data with other organisations.
- Caldicott 2 Review Report and Recommendations

Acknowledgements

Acknowledgements are given to The Princess Alexandra Hospitals NHS Trust who kindly shared the their Data Protection Impact Assessment Tools for use and adaptation by members of the Yorkshire and the Humber Strategic Information Governance Network (SIGN)

DPIA PROCESS

Appendix A



FOR OFFICE USE

ONLY REF:

DATED:

Appendix B

DPIA01 FORM: *DATA PROTECTION AND PRIVACY IMPACT SCREENING*

The following screening questions will help the IG Team decide whether a full data protection and privacy assessment is necessary. Your answers will provide an indication whether a full assessment must be undertaken.

Q1	The details of responsible lead to the project	Name	
		Title	
		Department	
		Telephone	
		E-mail	
Q2	The details of the Information Asset Owner	Name	
		Title	
		Department	
		Telephone	
		E-mail	
Q3	The name of the project/change		
Q4	Reference to project or scheme reference number where applic.		
Q5	Estimated completion date of project:		
Q6	Describe the project background, why has the project been initiated?		
Q7	Describe in a few sentences the benefits, quality expectations and intended outcomes:		
Q8	Describe the constraints to the project/change:		

Q9	Does the project include any of the following activities;	Retrieval, obtaining, recording or holding information or data
		Alignment, matching, combining, organisation, adaptation or alteration of information or data
		Consultation or use of information or data
		Blocking, erasure or destruction of information or data
	Q9 not applicable	Disclosure or sharing of information or data

Q10	Do the project/change activities include any of the following data sets;	**Personal identifiable details** (e.g. name, address, e-mail address, postcode, date of birth)
		Identifier numbers (e.g. NHS, national insurance, passport, driving license numbers)
		Genetic data (e.g. DNA, an individual's gene sequence)
		Biometric data (e.g. fingerprints, facial recognition, retinal scans)
		Family, lifestyle and social circumstances (e.g. marital status, housing, travel, leisure activities, membership of charities)
		Vulnerable individuals (e.g. refer to safeguarding policies)
		Education and training details (e.g. qualifications or certifications, training records)
		Employment details (e.g. career history, recruitment and termination details, attendance details, appraisals)
		Financial details (e.g. banking, income, salary, assets, investments, payments)
		Goods or services (e.g. contracts, licenses, agreements)
		Legal details (e.g. legal documents or agreements, court papers)
		Cultural identity including racial or ethnic origin
		Political opinions, religious or philosophical beliefs
		Health data (e.g. treatment, diagnosis, medical information including a physical or mental health or condition)
		Location data (e.g. GPS location, Wi-Fi tracking, vehicle tracking)
		Technology identifiers (e.g. device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags)
		Criminal proceedings (e.g. convictions, outcomes, sentences including offences or alleged offences)
	Q10 not applicable	**Sexual life** (e.g. sexual health, sex life or sexual orientation)

Q11	Does the project include any of the following activities;		**Evaluation or scoring, including profiling** (e.g. credit scoring, fraud protection, questionnaire's that generate a profile to an individual)
			Automated decision-making (where a decision is taken without human intervention e.g. automated system, algorithms)
			Direct marketing (e.g. newsletters, postcards, telemarking, e-mail subscriptions)
			Systematic monitoring of individuals (e.g. CCTV, body camera's, health data through wearable devices)
			Storing or transferring data outside the EU (e.g. cloud computing, accessing data outside the EU, use of an American transcribe company)
			Processing data on a larger scale (more than 11 individuals)
			Characteristic's which may affect an individual's legal rights or responsibilities ultimately preventing the exercise their rights or contract
			Implementation of a new technology, system or business process or collection of new information
			Change to existing technology, system or business process will significantly amend the way in which data or business is handled or used
			Use of a supplier

Q11 ***not applicable***

END OF DPIA01

DECLARATION

This DPIA01 form and declaration **must** be completed and returned to IGSharedService@calderdaleccg.nhs.uk by email, regardless whether a full data protection and privacy assessment was deemed to be necessary.

Upon the successful receipt the responsible lead to the project will receive a confirmation of receipt.

Responsible project lead	
Project name	
Project or scheme reference number	
Estimated project completion date	

◯ **None** of the screening questions within this document apply to the above project; therefore I feel that it is not necessary to conduct a full Data Protection and Privacy Impact Assessment.

◯ **Some** of the screening questions within this document apply to the above project; therefore, it is likely that a full Data Protection and Privacy Impact Assessment must be undertaken. I understand that at this stage the Data Protection Officer must be involved and the outcomes must be integrated into the project plan before the project is developed and implemented.

Signed:	
Dated:	

Appendix C

FOR OFFICE USE ONLY

REF:

DATED:

OUTCOME OF FULL DPIA

Following the evaluation of the DPIA01 form and declaration, a full data protection and privacy assessment was deemed to be necessary. The responsible project/service lead was notified that at this stage the Data Protection Officer (DPO) will now be involved and the DPO recommendation(s) and conclusions(s) must be integrated into the project plan before the project is developed and implemented.

Responsible project/service lead	
Project name	
Project or scheme reference number	
Estimated project completion date	

IDENTIFIED RISK(S)

SOURCES OF RISK(S)

RECOMMENDATION(S)

FINAL CONCLUSION(S)

By signing this DPIA outcome form, the responsible project/service lead confirms that they have read and understand the identified risk(s), sources of risk(s), recommendation(s) and conclusion(s) provided by the DPO. The responsible project lead is under no obligation to accept such recommendation(s) and conclusion(s) however under these circumstances, unaccepted recommendations and conclusions must have a rationale and be escalated to the SIRO.

◯ **ACCEPTED** The recommendations and conclusions will be integrated into the main project plan and actioned appropriately.

◯ **NOT ACCEPTED** The recommendations and conclusions will be integrated into the main project plan. However, they will not be accepted or actioned due to the following rationale:

Signed and dated:

Appendix D

Associated Documents to the DPIA Procedure

DPIA02 Supplier Requirements

DPIA02 Supplier Requirements_FINAL_

DPIA03 Lawfulness of Processing

DPIA03 Lawfulness of Processing_FINAL_

DPIA04 Data Quality

DPIA04 Data Quality_FINAL_v1.0.(

DPIA05 On-going Use of Data

DPIA05 On-Going Use of Data_FINAL_v

DPIA06 Technical and Security Measures

DPIA06 Technical Security Measures_FI

DPIA07 Systematic Monitoring, Automated Decision Making and Profiling

DPIA07 Systematic Monitoring Automatec

DPIA08 Disclosure and Sharing

DPIA08 Disclosure and Sharing_FINAL_v

Appendix E

Example risks

Risks to individuals

i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
ii. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
iii. New surveillance methods may be an unjustified intrusion on their privacy.
iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
vi. Identifiers might be collected and linked which prevent people from using a service anonymously.
vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
viii. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
x. If a retention period is not established information might be used for longer than necessary.

Corporate risks

i. Non-compliance with data protection or other legislation can lead to sanctions, fines and reputational damage.
ii. Problems which are only identified after the project has launched are more likely to require expensive fixes.
iii. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
iv. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
v. Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
vi. Data losses which damage individuals could lead to claims for compensation.

Compliance risks

i. Non-compliance with data protection legislation.
ii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
iii. Non-compliance with sector specific legislation or standards.
iv. Non-compliance with human rights legislation.

Appendix 3

Confidentiality Audit Procedure

Review and Amendment Log / Control Sheet

Responsible Officer:	Chief Finance Officer
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager
Date Approved:	April 2018
Committee:	Integrated Governance Committee
Version:	3.0
Review Date:	April 2020

Version History

Version	Date	Author	Description	Circulation
1.0	Nov 13	Associate IG Specialist WSYBCSU	Approved	Policy approved at Integrated Governance Committee on 21 November 2013
2.0	Dec 16	Senior Information Governance Officer	Approved	Added to Skyline
2.1	April 2018	Information Governance Manager	Draft	Review of procedure. Amendments to reflect changes under the General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017).
2.2	April 2018	Information Governance Manager	Draft	Policy and procedures approved by IGC subject to minor 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

Contents **Page**

Appendices

1. Introduction

1.1 This document sets out the procedure for carrying out audits relating to the access of person identifiable and business critical information for NHS Wakefield Clinical Commissioning Group (CCG)

1.2 The purpose of this procedure is to ensure that staff only access the records of individuals with whom they have a legitimate relationship or there is a legitimate business reason to access that information.

2. Aims and objectives

2.1 The objective of this procedure is to ensure that only appropriate staff access person identifiable level information and thereby:

a. Preserve integrity
   Protect the CCG's network from unauthorised or accidental modification of the organisation's information;

b. Preserve confidentiality
   Protect the CCG's information against unauthorised disclosure.

3. Scope of the Procedure

The procedure applies to all staff who work for the CCG including those on temporary or honorary contracts, secondments, pool staff, agency staff and students, and who have access to the CCG's information systems (including 3rd party staff). It also applies to relevant people who support and use these systems (IM&T staff).

All work areas within the CCG which process personal confidential information will be subject to the confidentiality audit procedures.

4. Accountability

4.1 The Governing Body

The Governing Body is accountable for ensuring that the necessary support and resources are available to protect the confidentiality of all patient information systems.

4.2 The Integrated Governance Committee

The Integrated Governance Committee is responsible for the review and approval of this procedure.

4.3 Accountable Officer

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

4.4 Senior Information Risk Owner

The SIRO has organisational responsibility for all aspects of Information Governance, including the responsibility for ensuring CCG has appropriate systems and policies in place to ensure that the organisation has robust information governance management. 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.

4.5 Caldicott Guardian

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient identifiable information. The Caldicott Guardian will ensure that any concerns and recommendations arising from the confidentiality audits are actioned within a reasonable timeframe.

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.

4.6 Data Protection Officer

The Date Protection Officer (DPO) is responsible for the provision of advice on the monitoring of data protection compliance which includes conducting assurance audits. 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.

4.7 IG Lead

The Governance and Board Secretary is the Information Governance Lead for the CCG and is responsible for ensuring effective management of confidentiality audit procedures. The Information Governance Team will support the IG lead to embed this procedure within the organisation.

4.8 Information Asset Owners

Information Asset Owners (IAO) are directly accountable to the SIRO and must support confidentiality audits of information assets they are responsible for.

4.9 Heads of Service

Heads of Service are responsible for ensuring that they and their staff are aware that confidentiality audits take place.

5. Definition of Terms

The words used in this procedure are used in their ordinary sense and technical terms have been avoided.

6. Procedure

6.1 Access to Regular Audit Trails

The Information Governance Lead supported by Information Governance Team will work together with the relevant IAO to annually run an audit trail for a systems holding person identifiable or business critical information. This work will be incorporated into the Information Asset Risk Management work plan.

The Information Governance Team will support the CCG to decide which systems audit trail to run and ensure this is included within the annual Information Assurance and Risk Management work programme.

6.2 Access to Ad-Hoc Audit Trails

If there a requirement to see which members of staff have accessed a particular record, where it is suspected that staff may have accessed the record when they do not have a legitimate relationship to do so then this may only be authorised by a Head of Service or above. See **Appendix A** of this procedure.

6.3 Information to be contained in the Audit Trail

The information to be contained within the audit will contain at minimum, the following:

- Failed attempts to access confidential information;
- Repeated attempts to access confidential information;
- Successful access of confidential information by unauthorised persons;
- Evidence of shared login sessions/passwords

6.4 Confidentiality/Information Governance Compliance Spot Checks

Information Governance Compliance spot checks around the offices of the CCG will be carried out once every 6 months to ensure staff are implementing information security controls and keeping confidential information sufficiently secured.

Areas to be audited include:

- Security applied to manual files, e.g. clear desks, storage in locked cabinets/locked rooms;
- Security applied to mobile equipment and desktops
- The location of fax machines and answer phones which receive confidential information
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information;
- Effective arrangements for retention and disposal of confidential information.

6.4 Reporting

If there are any suspicious findings from the audit trail then these will be immediately reported to the SIRO who will decide if further investigations should be carried out or disciplinary action taken.

The Information Governance Team will submit reports to the CCG IG Lead, the SIRO and Integrated Governance Committee highlighting their findings from the confidentiality audits.

7 Implementation and dissemination

Following approval by the Integrated Governance Committee this procedure will be disseminated to staff via the intranet and communicated through in-house newsletters.

8 Monitoring compliance with and the effectiveness of the procedure

Performance indicators will include:

Measurable Objective	Monitoring/ Audit	Frequency of monitoring	Responsibility for performing the monitoring
Audits are carried out on each CCG team/directorate	Completed Audits	Annual	Information Governance Manager
Individuals are complying with requirements to	Confidentiality Walk round	Twice yearly	Information Governance Manager

keep personal confidential data secure			
Individuals are complying with requirements to keep personal confidential data secure	Information Governance Staff Survey	Annual	Information Governance Manager
The organisation is mature in its understanding of Information Governance and reports breaches in an open an transparent way	Incidents Reported	Annual	Information Governance Manager

The performance against the indicators will be reported to the Integrated Governance Committee as part of the Information Security Assurance Report.

9 Questions

If you have any questions or comments about the Confidentiality Audit Procedure, please contact the Information Governance Lead. If you do not have any questions the CCG presumes that you understand and are aware of the rules and guidelines in this Confidentiality Audit Procedure and will adhere to them.

10 References

Copyright, Designs & Patents Act 1988
Computer Misuse Act 1990
General Data Protection Regulation (EU) 2016/679 and Data Protection Act (based on the Data Protection Bill 2017
The Human Rights Act 1998
Privacy and Electronic Communications (EC Directive) Regulations 2003
Regulation of Investigatory Powers Act 2000

11 Associated Documentation

Information Governance Policy and Framework
Confidentiality Policy and Data Protection Policy and Procedure
Incident Reporting Procedure
Records Management and Information Lifecycle Policy and Procedures
Disciplinary Policy

Appendix A

Request for an audit to be carried out as to which staff have accessed an individual's record

I authorise **XXXXXXXXXXX** to carry out an audit to ascertain which member(s) of staff have accessed a specific patient's record and on which dates

Name of person's record to be accessed ……..:

Individuals unique identifier i.e. NI / NHS Number…….

I believe that the member of staff has accessed the above individual's record when they did not have a legitimate right to do so.

Signed …….

Date……...

Name……..

Position……..

Appendix 4

Safe Haven Guidelines And Procedure

Review and Amendment Log/Control Sheet

Responsible Officer:	Chief Finance Officer
Clinical Lead:	Caldicott Guardian
Author:	Information Governance Manager / Governance and Board Secretary
Date Approved:	April 2018
Committee:	Integrated Governance Committee
Version:	3.0
Review Date:	April 2020

Version History

Version	Date	Author	Description	Circulation
1.0	December 2014	IG Associate / Governance & Board Secretary	Approved	Policy approved by Integrated Governance Committee on 18 December 2014
2.0	December 2016	Information Governance Manager	Approved	Added to Skyline
2.1	April 2018	Information Governance Manager	Draft	Review of procedure. 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

Contents **Page**

Safe Haven Guidelines and Procedure

1. Introduction

In order to comply with legislation and Department of Health guidance, all NHS organisations are required to have safe haven procedures to safeguard the privacy and confidentiality of personal or sensitive information both in transmission and storage.

These guidelines are intended to ensure that the transfer of personal and business confidential information both in and out of the organisation and between operational sites is as secure as possible.

The guidelines cover all categories of information and all staff groups as defined in associated polices including but not limited to the Records Management and Information Lifecycle Policy and Procedures and Confidentiality and Data Protection Policy and Procedures.

All routine flows of personal data and special category data either in or out of departments should be recorded within the register of transfers of personal information (data flow records).

2. Definitions

'Safe Haven'	a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the organisation to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the CCG whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles.
'Confidential Corporate Information'	All categories of corporate information should be regarded as confidential in the first instance although they may be releasable through the Freedom of Information regime including the Publication Scheme. This includes (but is not limited to): • Board and meeting papers and minutes • Tendering and contracting information • Financial and statistical information • Project and planning information

For definitions on 'Personal Data' and 'Special Category Data' please see the glossary of terms within the Confidentiality and Data Protection Policy and Procedures.

3. General Guidelines

Safe haven procedures should be in place in any location where personal information is being received, held or communicated especially where the information constitutes special category data.

3.1 Sending Confidential Information

Always consider first whether it is absolutely necessary to send confidential information and whether you have the necessary legal basis or permissions to do so.

4. Safe Haven Fax Machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules must apply:

- Ensure it is sited in an area that is restricted to those who need to access the information. This means a locked area or the use of password protection to send or print from the machine.
- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain that the correct person will receive it and that the fax number is correct.
- You must notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- The confirmation of receipt should be checked to ensure the fax has been transmitted to the intended recipient. Where possible this should be attached to the original document.
- Where possible the NHS number or another agreed identifier should be used for identification in preference to the patient's name and address.
- Care is taken in dialling the correct number.
- Confidential faxes are not left lying around for unauthorised staff to see
- Only the minimum amount of personal information should be sent.
- All confidential faxes sent should be clearly marked" Private and Confidential" on the front sheet.
- Frequently used numbers should be programmed into the fax machine 'memory dial' facility. This will minimise the risk of dialling incorrect numbers.
- A designated Safe Haven should be in a room/area where any incoming fax, letters or emails can be received in privacy and retrieved only by authorised personnel.

- If you receive a call requesting that confidential information be sent via fax always call the requestor back to confirm the caller's identity using an independent number source.
- Always seek advice from your line manager or the Information Governance team if you are unsure whether or not to send information via fax.
- If the correspondence is highly sensitive ensure someone is at the receiving end is waiting for it.
- Ensure only authorised staff handle confidential information.
- If you receive faxes that contain personal information store them in a secure environment.

5. Safe Haven Post

- Incoming mail should be opened away from public areas.
- Outgoing mail (both internal and external) should be sealed securely and marked private and confidential if it contains person-identifiable information.
- Where possible send post to a named person.
- When sending documents by external post or courier, use a "signed for" delivery service.
- Royal Mail offer a number of delivery services some of which offer a 'tracked' service:
    - **Standard Delivery** provides a free delivery confirmation service online. This service is not tracked.
    - **Confirmed** provides a 'signed for' service with delivery confirmation online. This service is not tracked.
    - **Tracked** provides end to end tracking online as well as delivery confirmation.

- Use appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the address is typed or written clearly in indelible ink.
- When sending outside of the NHS, send documents only to known, named, authorised personnel marked 'Confidential'.
- Use a risk assessment and register mail if appropriate.
- Refer to detailed guidance in Records Management and Information Lifecycle Policy and Procedures.
- In relation to sending subject access request responses by post, please additionally refer to the Subject Access Request and Access to Health Records Procedure.

6. Paper Documents in Use

- All sensitive records must be placed face down in public areas and not left unsupervised at any time.
- Information that is no longer required (e.g. post it notes, messages) should be shredded or disposed of under confidential condition.

- Keep a log of what records have left the department. Ensure that records are properly “booked out" of any relevant filing system if necessary, and that a record is kept of what is sent and where. Copies should be sent or retained, as appropriate.
- Refer to detailed guidance in the Records Management and Information Lifecycle Policy and Procedures.

7. Telephone calls

- Do not make telephone calls where you can be overheard (e.g. Reception)
- When you receive a call check to ensure you are speaking to the correct person, ring back (where possible) to confirm someone’s identity.

8. Physical Location and Security

- Do not allow unauthorised people into areas where confidential information is kept unless supervised. Ask to view peoples ID badges.
- Take measures to prevent casual scanning of information.
- Store person-identifiable information in a locked drawer/filing cabinet.

9. Computers and other IT Devices

- When transmitting or storing information electronically always follow the appropriate CCG policies, procedures and guidelines including, but not limited to the Electronic Communications and Social Media Policy and Procedure and Information Security Policy (incorporating Network Security).

10. Incidents

All incidents must be reported using the Incident Reporting Policy.

10.1 Fax Incidents

If a fax goes astray:

- Ask the recipient to shred the information which they have received.
- Make a note of the name and fax number of the unintended recipient.
- Register the incident on the Incident Reporting System.
- Review the risk to the person whose personal information has been disclosed or lost.
- Discuss immediately with your line manager and, where agreed, inform the person affected including any risk that you think has been caused.
- If the person affected is a service user, make a note in the relevant record stating how they were informed.
- Explain to the person affected how they can make a complaint, should they wish to do so.

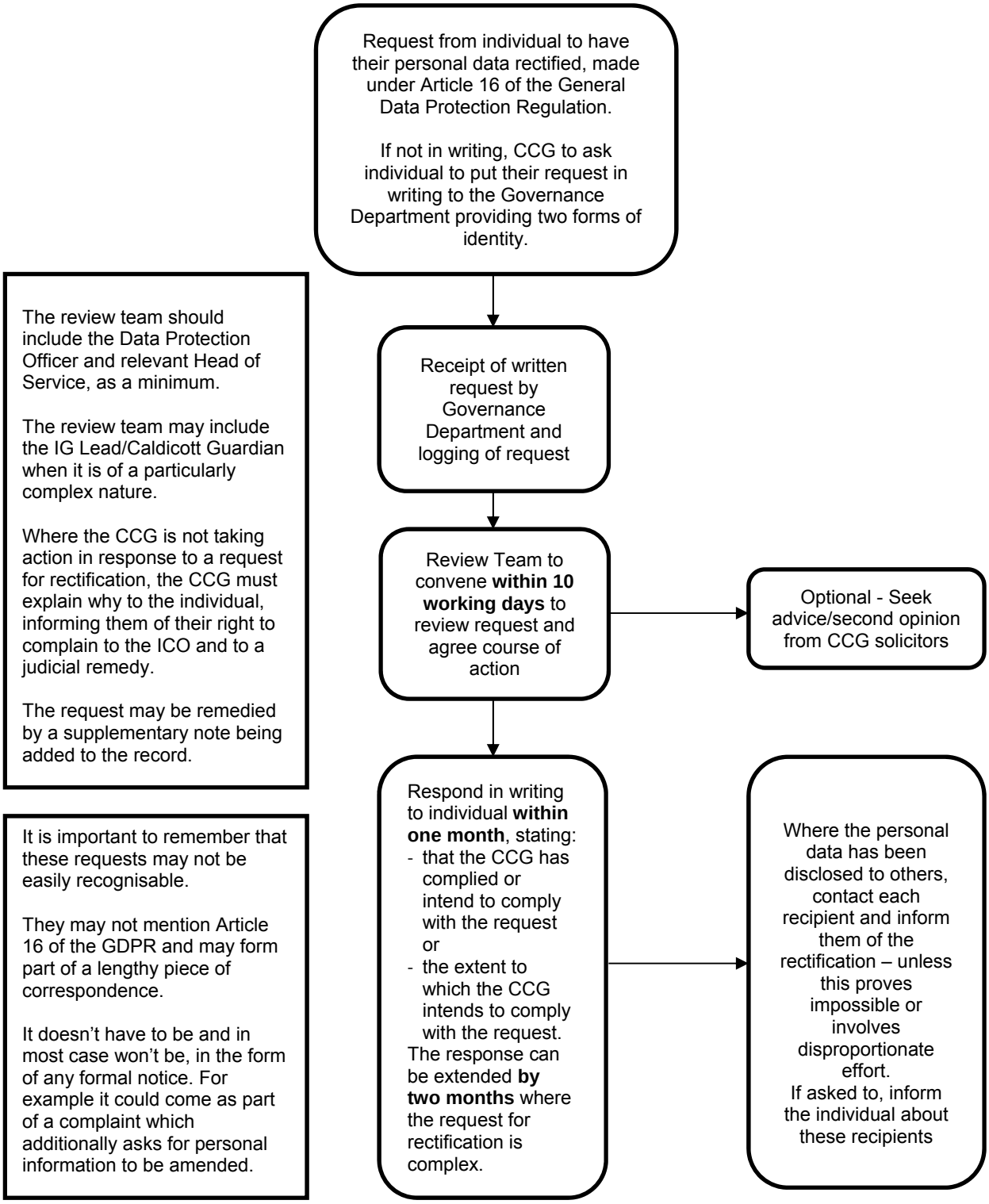
10.2 Postal Incidents

If post is lost or goes astray:

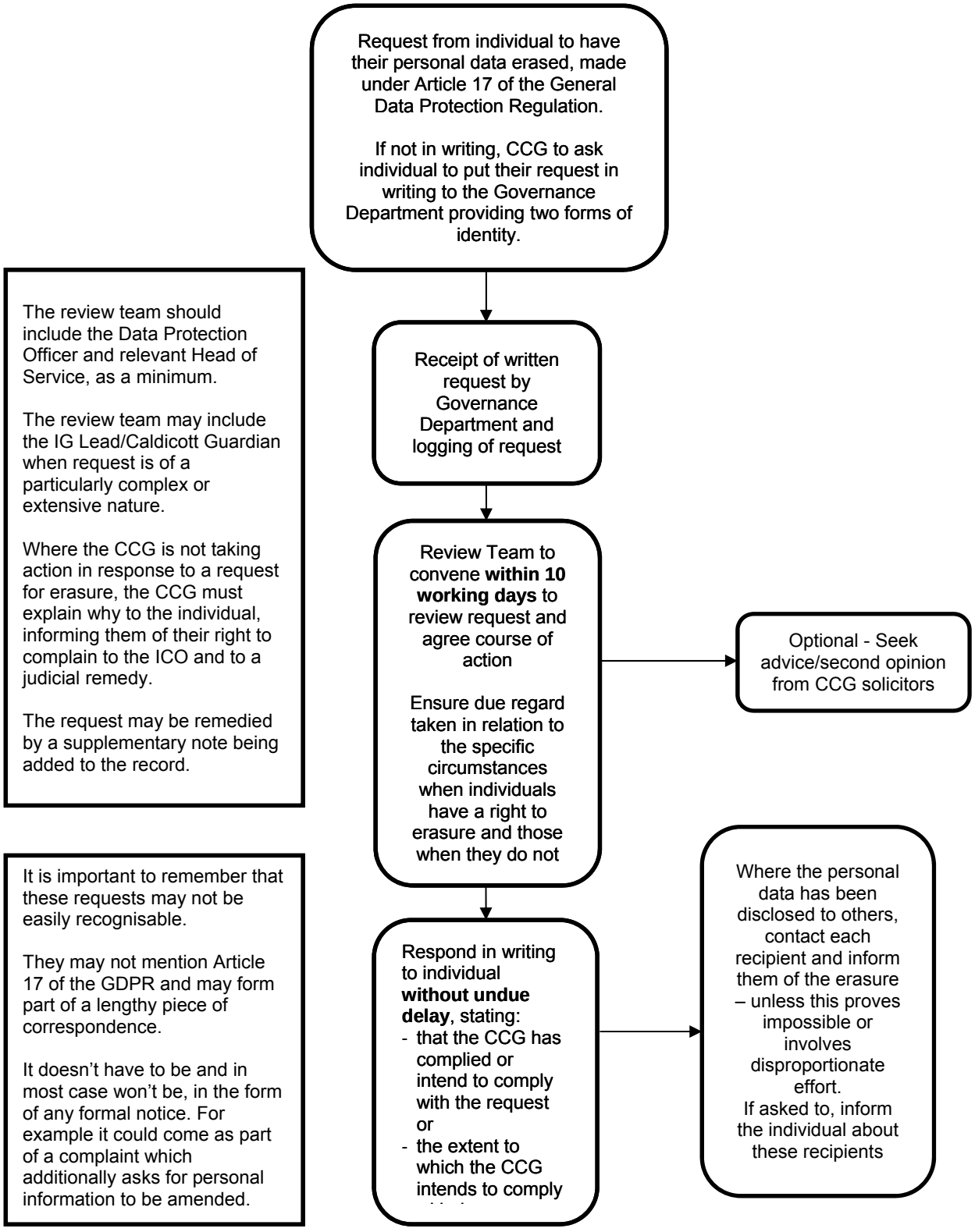
- Where known, arrange for the unintended recipient to return the information or files to the CCG. It may be most appropriate to arrange prompt collection.
- Review the risk to the person whose personal information has been disclosed or lost.
- Register the incident on the Incident Reporting System.
- Discuss immediately with your line manager and, where agreed, inform the person affected, including any risk that you think has been caused.
- If the person affected is a service user make a note in the relevant record stating how they were informed of the loss of information.
- Explain to the person affected how they can make a complaint, should they wish to do so

Appendix 5

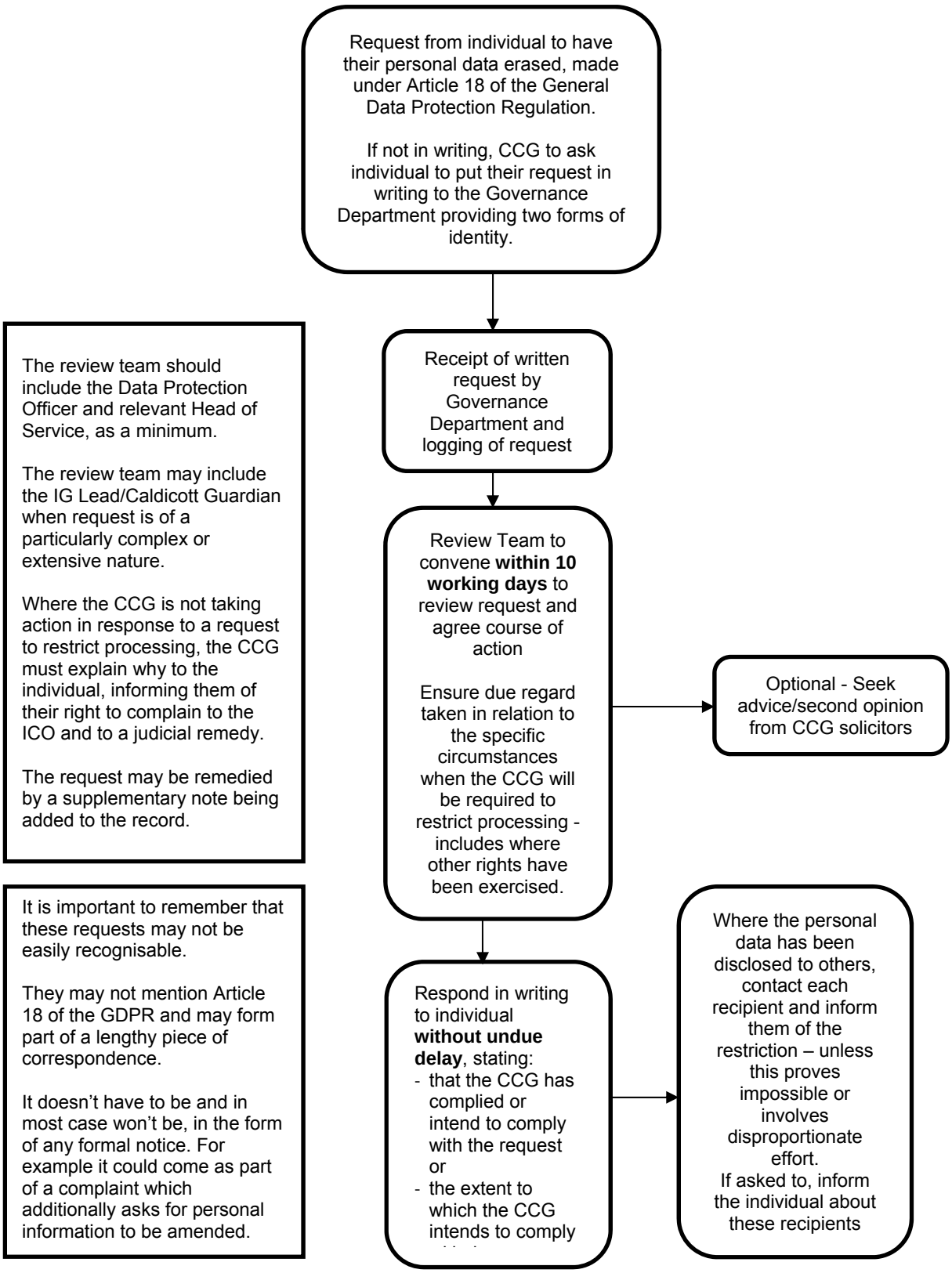
Process Flow Chart – Process for Managing Requests under the Right to Rectification



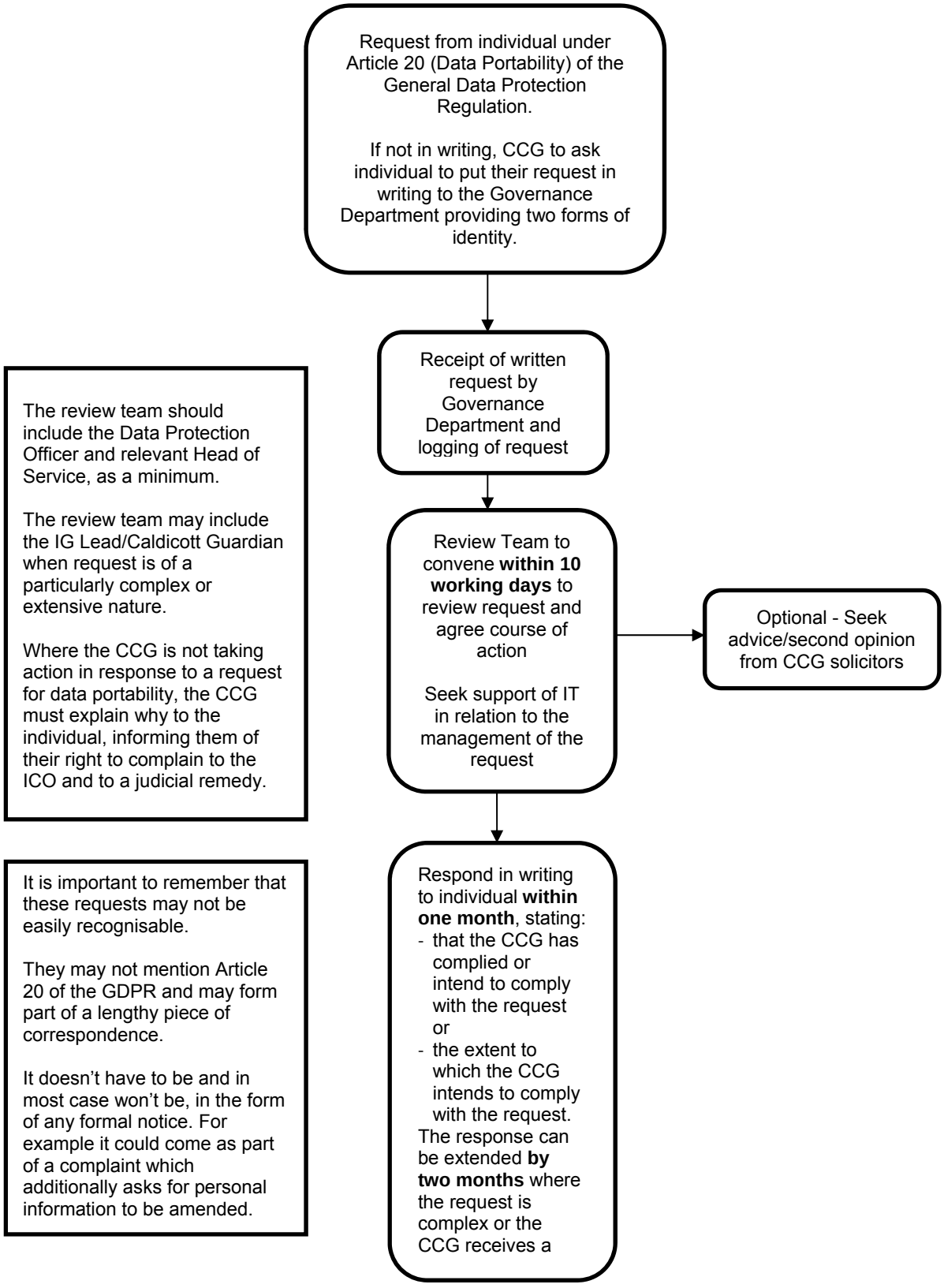
Process Flow Chart – Process for Managing Requests under the Right to Erasure



Process Flow Chart – Process for Managing Requests under the Right to Restrict Processing



Process Flow Chart – Process for Managing Requests for Data Portability



Process Flow Chart – Process for Managing Requests under the Right to Object