NHS
Derby and Derbyshire
Clinical Commissioning Group

NHS Derby and Derbyshire Clinical Commissioning Group

Information Governance (IG) Policy

KEY POLICY MESSAGES	
1.	Confidentiality, availability and integrity of all information held and used by, or on behalf of the CCG must therefore be assured
2.	Under data protection legislation, the CCG must be able to demonstrate its compliance with the legislation
3.	All staff members are responsible for maintaining compliance with the data protection principles and the General Data Protection Regulation (GDPR), completing their Data Security and Protection training annually, and for reporting non-compliance through the CCG incident reporting process

VERSION CONTROL

Title:	NHS Derby and Derbyshire CCG Information Governance (IG) Policy
Supersedes:	• IG01 – IG Management Framework • IG02 – IG Policy • IG03 – Staff IG Code of Conduct • IG09 – IG Training Plan • IG14 – IG Staff Handbook • IG16 – Confidentiality and Data Protection Policy
Description of Amendment(s):	Version 1.0 – Initial Draft Version 2.0 – June 2020. Reviewed July 2020 Version 3.0 – Version number updated following approval at Governance Committee November 2020. Version 3.1 – Compliance statement added to Target Audience.
Financial Implications:	Not Applicable
Policy Area:	Corporate Delivery
Version No:	Version 3.1
Author:	IG Team (Ruth Lloyd, Information Governance Manager & Emma Holt, Information Governance Assistant)
Approved by:	Governance Committee, 12 November 2020
Effective Date:	November 2020
Review Date:	November 2022
List of referenced policies	IG02: NHS Network, Internet and Electronic Mail Acceptable Use Policy IG03: Records Management Policy IG04: Subject Access Procedure
Key Words section (metadata for search facility online)	Information Governance Data Protection Confidentiality Staff responsibilities Breach reporting
Reference Number	IG01
Target Audience	CCG approved policies apply to all employees, contractors, volunteers, and others working with the CCG in any capacity. Compliance with CCG policy is a formal contractual requirement and failure to comply with the policy, including any arrangements which are put in place under it, will be investigated and may lead to disciplinary action being taken.

CONTENTS

1. BACKGROUND

1.1 This policy applies to NHS Derby and Derbyshire Clinical Commissioning Group, subsequently referred to in this document as the CCG.

1.2 Definition of Information Governance (IG) in the NHS:

1.2.1 IG is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.2.2 It provides a way for employees to deal consistently with the many different information handling requirements including those set out in the:

- Data Protection Act 2018
- General Data Protection Regulation (GDPR)
- Common law duty of confidentiality
- Confidentiality: NHS code of practice guidelines
- Information security: NHS code of practice guidelines
- Records management: NHS code of practice guidelines
- Freedom of Information Act 2000
- Human Rights Act
- Health and Social Care Act 2012

1.3 The CCG depends on the use and flow of information and data to meet its mandate of planning and commissioning of health care services within its local area.

1.4 The confidentiality, availability and integrity of all information held and used by, or on behalf of the CCG must therefore be assured. This requires robust Information Governance in order to:

1.4.1 support delivery, service planning and performance;

1.4.2 enable the effective management of services and resources;

1.4.3 ensure that all types of information in all formats are sourced, held and used appropriately, securely and legally;

1.4.4 protect privacy and confidentiality;

1.4.5 ensure the effective application of Information Security standards and behaviours throughout the CCG through a defined set of accountabilities;

1.4.6 maintain public trust.

1.5 This policy describes the accountability framework for handling information in a confidential and secure manner to the appropriate professional and quality standards required of a modern health service. It brings together independent yet

associated requirements and standards of practice, including people, policies, processes and technology.

1.6 The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian's ten security standards. These are the basis of the Data Security and Protection Toolkit that the CCG must use to assess its IG performance.

1.7 Under data protection legislation, the CCG must be able to demonstrate its compliance with the legislation. The arrangements set out in this policy are intended to achieve this compliance.

2. PURPOSE

2.1 The purpose of this policy is to provide the over-arching framework within which all Information Security issues shall be conducted and managed. It is to ensure that all CCG information assets are protected to a consistently high standard including manual and electronic records, and both patient and corporate information, and to define a clear set of accountabilities in ensuring that protection.

2.2 This policy establishes employee responsibility and the rules of conduct for all members of staff regarding the IG agenda for the CCG. It covers the following content:

- Information Governance Management Framework (IGMF)
- Roles and Responsibilities
- Confidentiality and Data Protection
- Information Security
- Incident Reporting
- Data Security and Protection Toolkit
- IG Training

The policy intends to set out the approach of the organisation to provide a robust IG management framework for the current and future management of Information and compliance with required legislation.

3. SCOPE

3.1 This policy applies to all staff within the CCG (whether operating directly or providing services to other organisations under a service level agreement, or joint agreement), and to non-executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.

3.2 **Definitions**

"Consent"

means any freely-given specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed;

"Data Controller"

means the person or the organisation that collects personal data and decides on how to use, store or distribute that data;

"Data Processor"

means any person or organisation (other than an employee of the data controller) that processes personal data on behalf of the data controller

"Data Subject or Natural Person"

means an individual who is the subject of the personal data;

"Personal Data"

means any information held about an individual who can be identified from that information. For example, name, address, postcode, NHS number, etc. Any personal data must be treated as confidential;

"Special Category Data"

means processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited;

4. INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

4.1 The Information Governance Management Framework (IGMF) provides a summary/overview of how the CCG is addressing the IG agenda and reflects the capacity and capability of the CCG. See Appendix 1.

4.2 The Reporting Structure is included in this policy as Appendix 2.

5. ROLES AND RESPONSIBILITIES

5.1 Accountable Officer

5.1.1 Overall accountability across the organisations lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective information governance assurance framework for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.1.2 The CCG has established a control and reporting framework for information governance as detailed in 3.1.

5.1.3 The Governing Body is accountable for the overall CCG compliance with information governance related legislation, including the Data Protection Act 2018. The Governing Body has nominated the Chief Nurse for Caldicott, the Medical Director as Data Protection Officer, and the Executive Director of Strategy and Delivery as Senior Information Risk Owner. All roles are supported with a formal letter of delegation from the Chief Officer.

The CCG Board Assurance Framework includes the risk relating to the CCGs compliance with Information Governance, and this is regularly reviewed, with the CCG Governing Body setting the risk appetite of the organisation.

5.2 All Staff

5.2.1 All staff must adhere to the CCG's policies and procedures relating to the processing of personal information. It is part of employment contracts once signed that all staff agree to abide by organisational policies, and this includes all IG policies, before accessing any data or systems provided by the CCG. The CCG policies represent the CCGs standards for Acceptable Use.

5.2.2 All staff members are responsible for maintaining compliance with the data protection principles and the General Data Protection Regulation (GDPR), completing their Data Security and Protection training annually, and for reporting non-compliance through the CCG incident reporting process.

5.2.3 All staff are reminded of the Data Subjects right to confidentiality, noting that decisions to set aside the common law duty of confidentiality are to be made in discussion with the Caldicott Guardian, in order to ensure lawful processing of data, and that the reputation of the CCG is upheld.

5.2.4 The common law duty of confidentiality is explained below:

> *The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.*

In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client.

5.3 **Line Managers**

Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their group or directorate.

5.4 **Information Governance (IG) Lead**

The IG Lead will:

5.4.1 develop and maintain comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures.

5.4.2 promote compliance across the CCG staff base with the IG policies on behalf of the SIRO.

5.4.3 ensure that there is senior management awareness and support for IG resourcing and implementation of improvements.

5.4.4 provide direction in formulating, establishing and promoting IG policies, via newsletters, staff communications, web content, leaflets and face to face training.

5.4.5 establish working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.

5.4.6 ensure that assessment and improvement plans are prepared for approval by the senior level of management in a timely manner and in line with national reporting requirements.

5.4.7 ensure that the approach to information handling is communicated to all staff and made available to the public, via the publication of privacy notices;

5.4.8 ensuring that appropriate training is made available to staff and completed as necessary to support their duties and in line with the DSPT requirements and as detailed in the CCG's Training Needs Analysis;

5.4.9 liaise with other committees, working groups and programme boards in order to promote and integrate IG standards;

5.4.10 monitor information handling activities to ensure compliance with law and guidance;

5.4.11 provide a focal point for the resolution and/or discussion of IG issues;

5.4.12 undertake annual training required by the role as identified in the CCG Training Needs Analysis.

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

The SIRO will:

5.5.1 oversee the organisation's information risk policy and information risk management strategy. All key information assets will be identified and their details included in an Information Asset Register;

5.5.2 oversee the risk assessment process for information and cyber security risks, including review of an annual information risk assessment to support and inform the Annual Governance Statement. This will include ownership of information and cyber security risks included within the board assurance framework;

5.5.3 work with the Chief Information Officer (CIO) and Chief Technology Officer (CTO) to ensure that delivery of information and cyber activities are assured as compliant with relevant data and privacy legislation;

5.5.4 approve and appoint IAOs, and ensure that each of these appointments are supported by a formal letter of delegation;

5.5.5 receive assurance that Information Asset Owners (IAOs) will be identified for each key information asset and that all systems information assets have an assigned information asset owner;

5.5.6 receive assurance that all staff assigned responsibility for co-ordinating and implementing information risk management will be appropriately trained to carry out their role;

5.5.7 approve the information flow mapping report and receive assurance that in-year each IAO carries out risk reviews of the assets for which they are accountable, the frequency of review depending upon the importance of the asset and the nature of the risk environment but at least annually;

5.5.8 to lead the Governance Committee's activities to seek assurance of the effectiveness of risk management across the organisation;

5.5.9 undertake annual training required by the role as identified in the CCG Training Needs analysis;

5.5.10 to be added to and maintain registration on the National Register of SIROs;

5.5.11 the SIRO's accountabilities as described above are included in a formal letter of delegation from the Chief Officer.

5.6 **Data Protection Officer (DPO)**

The DPO will:

5.6.1 oversee and provide assurance that the organisation and its employees are receiving sufficient information and training to understand their data protection obligations under the GDPR;

5.6.2 receive assurance of compliance with the GDPR and internal data protection policies and procedure operation. This will include oversight of awareness training compliance and training of staff involved in processing operations (IAOs);

5.6.3 advise regarding stage two Data Protection Impact assessments (DPIAs), where high risk processing is identified, and provide a view on the manner of their implementation and outcomes;

5.6.4 serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting;

5.6.5 receive assurance that effective processes are in place for data subjects to respond to Subject Access request, and act as an escalation point where required;

5.6.6 ensure that appropriate confidentiality is maintained in the performance of his or her tasks;

5.6.7 delegate operational involvement in procurement tasks to the IG manager, retaining oversight and risk management as required;

5.6.8 oversee the overall GDPR compliance agenda, and assure the processes with regard to Data Protection Impact Assessment and policy application and review;

5.6.9 undertake annual training required by the role as identified in the CCG Training Needs analysis.

5.7 **Caldicott Guardian**

The Caldicott Guardian will:

5.7.1 oversee development and implementations of procedures, which ensure that all routine uses of person-identifiable patient information are identified, agreed as being justified and documented;

5.7.2 ensure that the priorities as detailed by the National Data Guardian 10 Data Security Standards are applied as a key function of their role;

5.7.3 oversee development and implementation of criteria and a process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes;

5.7.4 ensure standard procedures and protocols are in place to govern access to person-identifiable patient information;

5.7.5 understand and apply the principles of confidentiality and data protection as set out in the DH publication 'Confidentiality: NHS Code of Practice' and where current practice falls short of that required, to agree challenging and achievable improvement plans;

5.7.6 provide oversight of standard information governance procedures and protocols, ensuring that these are communicated in an understandable format and available to all staff;

5.7.7 ensure that planned activities are in place which provide opportunities for staff to raise awareness of the Caldicott Guardian and the overall IG agenda, through training and education. Education will include the standards of good information governance practice, Caldicott principles and to the principles of information sharing lawfully under the GDPR;

5.7.8 work with other care providers and linked agencies to facilitate better sharing of relevant information about patients in a manner which facilitates joined up care across institutional boundaries, while ensuring that patients' legal rights and the Caldicott Principles are maintained. The Caldicott Guardian is the signatory of information sharing agreements between the CCG and its contractors / partners;

5.7.9 ensure establishment of Information Sharing Protocols, in line with information provided by the Department of Health, to govern the use and sharing of patient-identifiable information between organisations both within and outside the NHS. The Caldicott Guardian will seek input from the IG Manager to provide assurance regarding the operational detail of each information sharing / processing agreement;

5.7.10 in collaboration with the Information Governance Manager, draw to the attention of all staff through raising general awareness (CCG wide bulletins, Team Brief and any other suitable means at disposal) correct practices in relation to person-identifiable patient information, following specific incidents where procedures, guidelines and protocols have been breached by staff;

5.7.11 undertake annual training required by the role as identified in the CCG Training Needs analysis.

5.8 Information Asset Owner (IAO)

5.8.1 IAOs must be senior/responsible individuals involved in running the relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why.

5.8.2 As a result they are able to understand and address risks to the information, and ensure that information is processed within the law. Information Asset Administrators (IAAs) are the deputies for the IAOs and are usually Department

Managers. The IAA ensures that staff adhere to policies and procedures which ensure the Confidentiality, Integrity and Availability of data in use in the CCG, and that any changes to processes within the department are reflected in the information flow mapping.

5.8.3 The IAA must consult their IAO on any potential or actual risks to the asset and ensure that information asset registers are accurate and up to date.

5.8.4 Annually as a minimum, the IAO must affirm to the SIRO that the processing they are undertaking is mapped, and risk assessed, with appropriate mitigations to any risks identified in place.

5.8.5 The IAO will:

(a) understand which 'assets' are in use by their staff / departments which they own;

(b) lead and foster a culture that values, protects and understands the importance of information;

(c) know what information the asset holds, and what enters and leaves it and why;

(d) know who has access and why, and ensure their use of the asset is monitored;

(e) understand and address risks to the asset, and provide assurance to the SIRO;

(f) ensure processes are in place for Subject Access where this is applicable;

(g) undertake annual training required by the role as identified in the CCG Training Needs analysis;

(h) each IAO will receive a formal letter of delegation from the SIRO, explaining the above responsibilities, noting that the overall accountability for information assets and their management sits with the SIRO.

6. CONFIDENTIALITY AND DATA PROTECTION

6.1 Data Protection Law

6.1.1 The CCG has a legal duty to comply with the General Data Protection Regulation (GDPR), the Data Protection Act 2018. The requirements of the Common Law Duty of Confidentiality must also be met.

6.1.2 The Common Law Duty of Confidentiality states that: "Information given or received in confidence, obtained for one purpose, must not be disclosed or used for another purpose without the consent of the provider of the information."

6.1.3 Article 5 of the GDPR requires that data controllers ensure personal data shall be:

(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;

(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.

6.1.4 Article 5 (2) requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.” This is called the Accountability Principle.

6.2 Individual Rights

Under Chapter 3 of the GDPR, Data Subjects have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling

6.3 **Confidentiality**

6.3.1 All employees of the CCG are responsible for maintaining confidentiality of staff and patients, and this duty of confidentiality is written into employment contracts.

6.3.2 Under normal circumstances staff do not have access to personal confidential data however where that is required as part of their role, and where there is a legal basis for handling the data, staff should ensure the basic principles of Data Protection and Caldicott are upheld. Accessing data that is not needed to carry out work or passing data to someone who is not authorised to receive it is a breach of confidentiality which could result in disciplinary action and organisational fines.

6.3.3 Staff must be mindful that confidential data will include: patient information; staff information; corporate information; and business sensitive information.

6.4 **Caldicott Principles**

Caldicott Principles look at the balance between safeguarding patients' sensitive information and encouraging responsible information sharing. Staff must follow the seven principles:

6.4.1 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.

6.4.2 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).

6.4.3 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.

6.4.4 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.

6.4.5 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.

6.4.6 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.

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

7. INFORMATION SECURITY

Reasonable care should be taken to protect the physical security of confidential data from accidental loss, damage or destruction and from unauthorised or accidental disclosure. Below are the CCG's Information Security Principles:

7.1 maintenance of passwords and the security of passwords is a personal responsibility;

7.2 staff must not write down passwords – to do so creates an unacceptable organisational risk both for system and building security;

7.3 staff must not share passwords with anyone else;

7.4 security badges must be worn and challenge provided for those without;

7.5 do not use someone else's password to gain access to information held on computers;

7.6 no person identifiable data should be held on any mobile devices (e.g. laptops, PDA's, memory sticks) unless it is encrypted to the approved standard (contact IT for encryption to be installed on devices containing person identifiable information);

7.7 faxing is not secure and should not be undertaken. Faxing in the NHS will be unlawful from April 2020;

7.8 envelopes containing confidential data must be securely sealed, labelled 'confidential' and clearly addressed to a known contact. Recorded delivery or courier will be used where required;

7.9 telephone validation procedures must be followed to confirm the identity of callers and their availability to receive information before information is given to them;

7.10 staff must always ensure that encypted transfer is in place (e.g. NHS Mail) when sending person identifiable data by email both inside and outside of the CCG;

7.11 staff must ensure that risks from cyber threats are reduced by following the guidance set out in training and the IG communications that are circulated and published;

7.12 staff must follow the CCG's policies and procedures relating to Data Protection, confidentiality, information security and seek advice when in doubt.

8. INCIDENTS AND BREACHES

8.1 Any breach of confidence, security incident, near miss or data loss can result in major consequences both for the staff member concerned, and the organisation, but mostly for people to whom the information relates (staff, patients or other members of the public).

8.2 Serious data losses can result in loss of public confidence in NHS services and could lead to legal action being taken against the organisation. It is possible that disciplinary action will be taken against staff for failure to comply with responsibilities in accordance with organisation policies, contractual expectations or professional codes of conduct.

8.3 Incident Reporting

8.3.1 All incidents and near misses must be reported to line managers and the IG Team as soon as possible after the event. An incident or near miss could include letters or emails sent to the wrong individual or received in the incorrect department.

8.3.2 Staff must follow the Incident Reporting procedure. See Appendix 3a and 3b.

8.4 Information Security Incident Management

8.4.1 <u>Definitions</u>

"Near Miss"

means where a security event has been identified, however upon investigation there is no present threat;

"Non-Incident"

means where someone has incorrectly considered something as a security event. However the action taken isn't a security event at all as there's been no breach of information security policy or failure of safeguards. For example sending an email to an incorrect address however the email contains no OFFICIAL information at all;

"Security Breach"

a security breach is where a security incident in which sensitive, protected or confidential data / system (i.e. OFFICIAL-SENSITIVE) is copied, transmitted, viewed, stolen or used/amended by an individual unauthorised to do so.

"Security Event"

means an identified occurrence of a system, service/process or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation which may be security relevant;

"Security Incident"

means a single or a series of unwanted or unexpected security events that have a significant probability of a present threat, compromising business operations and threatening information security;

NO EVENT = NON INCIDENT

EVENT + THREAT = INCIDENT

EVENT - THREAT = NEAR MISS (INCIDENT)

INCIDENT + COMPROMISE = BREACH

8.4.2 Staff must follow the Information Security Incident Management process. See Appendix 3C.

9. DATA SECURITY AND PROTECTION TOOLKIT

9.1 The Data Security and Protection Toolkit (DSPT) is a self-assessment tool, which NHS organisations are required to complete on an annual basis. The DSPT is developed and maintained by NHS Digital and provides a standard for information governance requirements for the NHS. The DSPT requires organisations to assess themselves against requirements for:

9.1.1 management structures and responsibilities, including staff training;

9.1.2 confidentiality and data protection;

9.1.3 information security.

9.2 The organisation is audited annually against the DSPT compliance to ensure that information is managed correctly, and that it is protected against unauthorised access, loss, damage and destruction. If the organisation fails to meet any of the required standards, an action plan will be required to achieve the standard within an 'acceptable timescale'. Such action plans are subject to agreement with NHS England and will be monitored by internal audit.

9.3 The CCG will work to maintain their DSPT status of 'standards met'.

9.4 **National Data Security Standards**

The CCG must commit to the following data security standards:

9.4.1 all staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes;

9.4.2 all staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches;

9.4.3 all staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit;

9.4.4 personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals;

9.4.5 processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security;

9.4.6 cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection;

9.4.7 a continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management;

9.4.8 no unsupported operating systems, software or internet browsers are used within the IT estate;

9.4.9 a strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually;

9.4.10 IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

10. TRAINING

10.1 To ensure organisational compliance with the law and central guidelines relating to IG, staff must receive appropriate training. Therefore, annual IG training is mandatory for all staff, including new starters, locums, temporary staff, lay members, student and contract staff members.

10.2 IG training needs are reviewed annually, routinely assessed, monitored and adequately provided for. IG knowledge and awareness should be at the core of the organisation's objectives, embedded amongst other governance initiatives and should offer a stable foundation for the workforce. Without this knowledge the ability of an organisation to meet legal and policy requirements will be severely impaired.

10.3 Data Security and Protection Training

10.3.1 All staff are required to undertake the mandatory 'Information Governance Data Security Awareness' Level 1 training module. This module is available either through ESR, online through e-lfh or the NHS Digital Workbook. Face to face training will be offered where necessary and as agreed by the Information Governance Assurance Forum.

10.3.2 Any member of staff completing the training through the e-lfh website will need to send a copy of their training certificate to the ESR team 'ddccg.esr@nhs.net'.

10.3.3 Completed training assessments should be submitted to the IG Team ddccg.igteam@nhs.net for marking and recording against the CCG training log.

10.3.4 The CCG's IG Team has produced a training presentation which mirrors the content of the NHS Digital Data Security Awareness Level 1 Training. The IG Team will deliver face to face training sessions where online training is not the preferred option. This will provide an alternative method of training ensuring training opportunities are fully inclusive reflecting the CCG's commitment to diversity. Additionally the face to face training will support members of staff identified as not possessing the required IT skills to complete the training on-line or where staff don't have regular access to computers.

10.3.5 There may be occasions when ad hoc training will need to be delivered by the IG Team to CCG staff based on an identified need, for example, changes in working practices following an incident.

10.4 Assessing Training Needs

10.4.1 Staff inevitably have different levels of awareness of their responsibilities for safeguarding confidentiality, protecting data and preserving information security.

In most cases the mandatory basic training will be sufficient to give staff the knowledge they require.

10.4.2 In order to fully meet the Data Security & Protection Toolkit Standard 3 the organisation has established a 'training needs analysis' (TNA) that identifies those additional training modules that need to be completed by specific staff groups or job roles. See Appendix 4.

10.4.3 The TNA identifies the training modules that are mandatory, or optional for specific staff groups or job roles to complete. It also addresses the frequency of the training and how training needs beyond the basic level will be assessed.

11. EQUALITY AND DIVERSITY

11.1 The CCG aims to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

11.2 This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

11.3 In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

12. DUE REGARD

12.1 The CCG aims to design and implement policy documents that meet the diverse needs of our services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all. The document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to socio-economic status, immigration status and the principles of the Human Rights Act.

12.2 In carrying out its function, the CCG must have due regard to the Public Sector Equality Duty. This applies to all activities for which the CCG is responsible, including policy development, review and implementation.

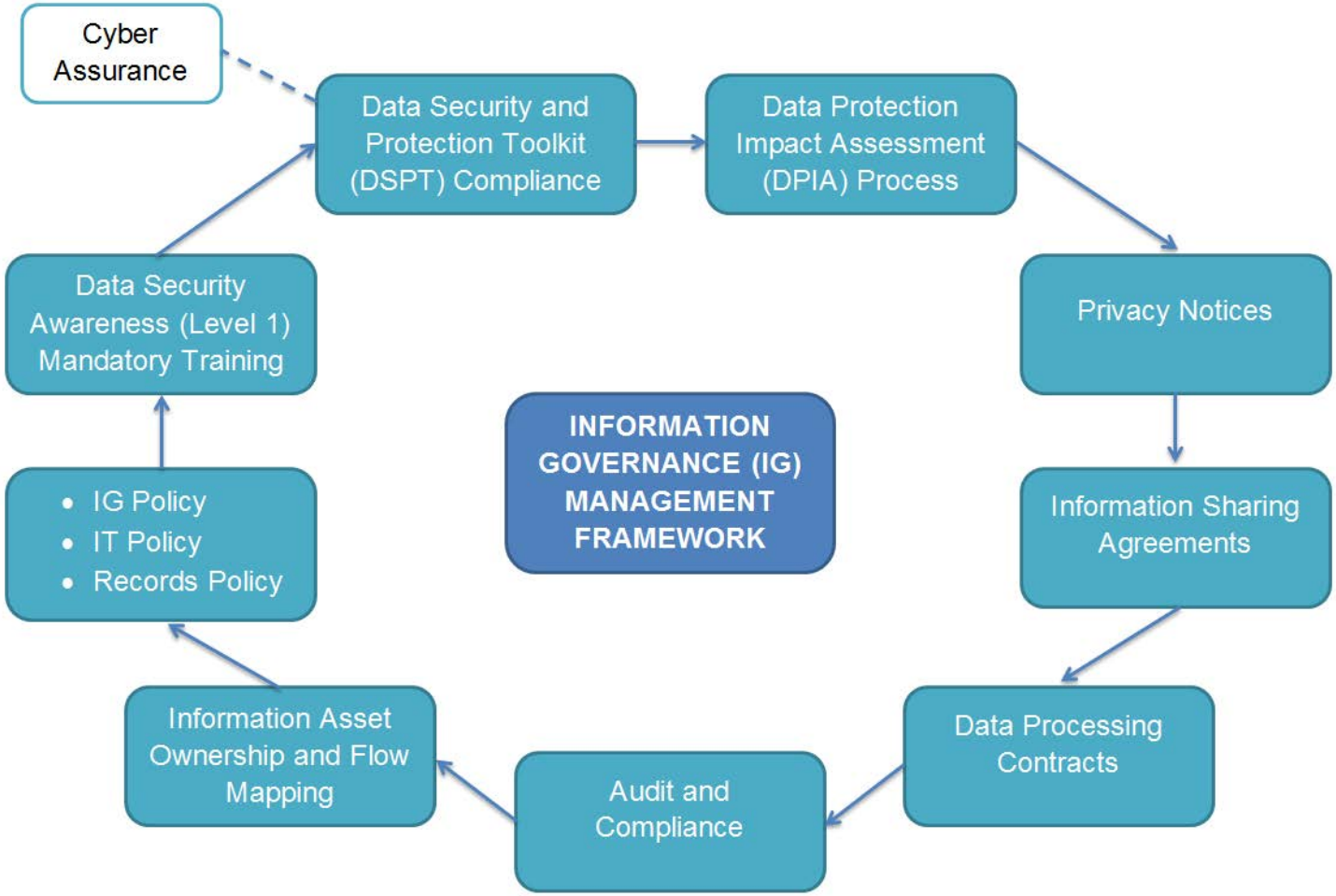
13. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Data Security and Protection Toolkit, will be undertaken each year. This includes confidentiality and data protection incidents that are reported.

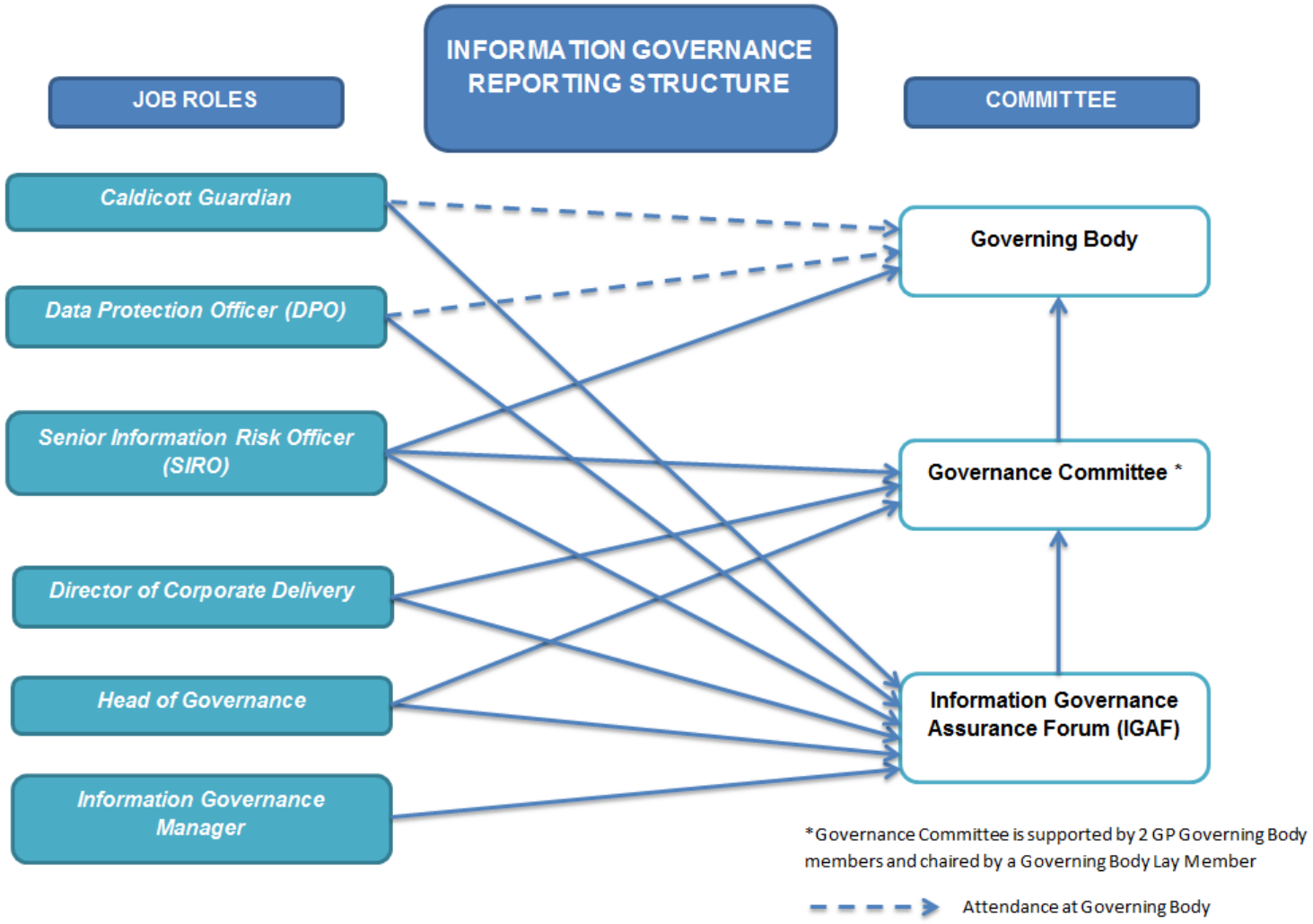
14. REFERENCES

- NHS Information Governance: Guidance on Legal and Professional Obligations https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations
- Handbook to the NHS Constitution https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england
- Confidentiality: NHS Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- Data Security and Protection Toolkit https://dsptoolkit.nhs.uk
- NHS Care Record Guarantee http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf
- Information Security Management: NHS Code of Practice http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf
- Records Management Code of Practice for Health & Social Care 2016 https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga
- Caldicott Guardian Manual 2017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
- NHS Digital Guide to the Notification of Data Security & Protection Incidents. Sept 2018 https://www.dsptoolkit.nhs.uk/Help/29
- NHS Information Risk Management http://systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf
- The Caldicott Review: Information Governance in the Health and Social Care System https://www.gov.uk/government/publications/the-information-governance-review
- General Data Protection Regulations 2016 https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
- The Data Protection Act 2018 https://ico.org.uk/for-organisations/data-protection-act-2018
- Your Data: Better Security, Better Choice, Better Care https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf

Appendix 1 – Information Governance Management Framework

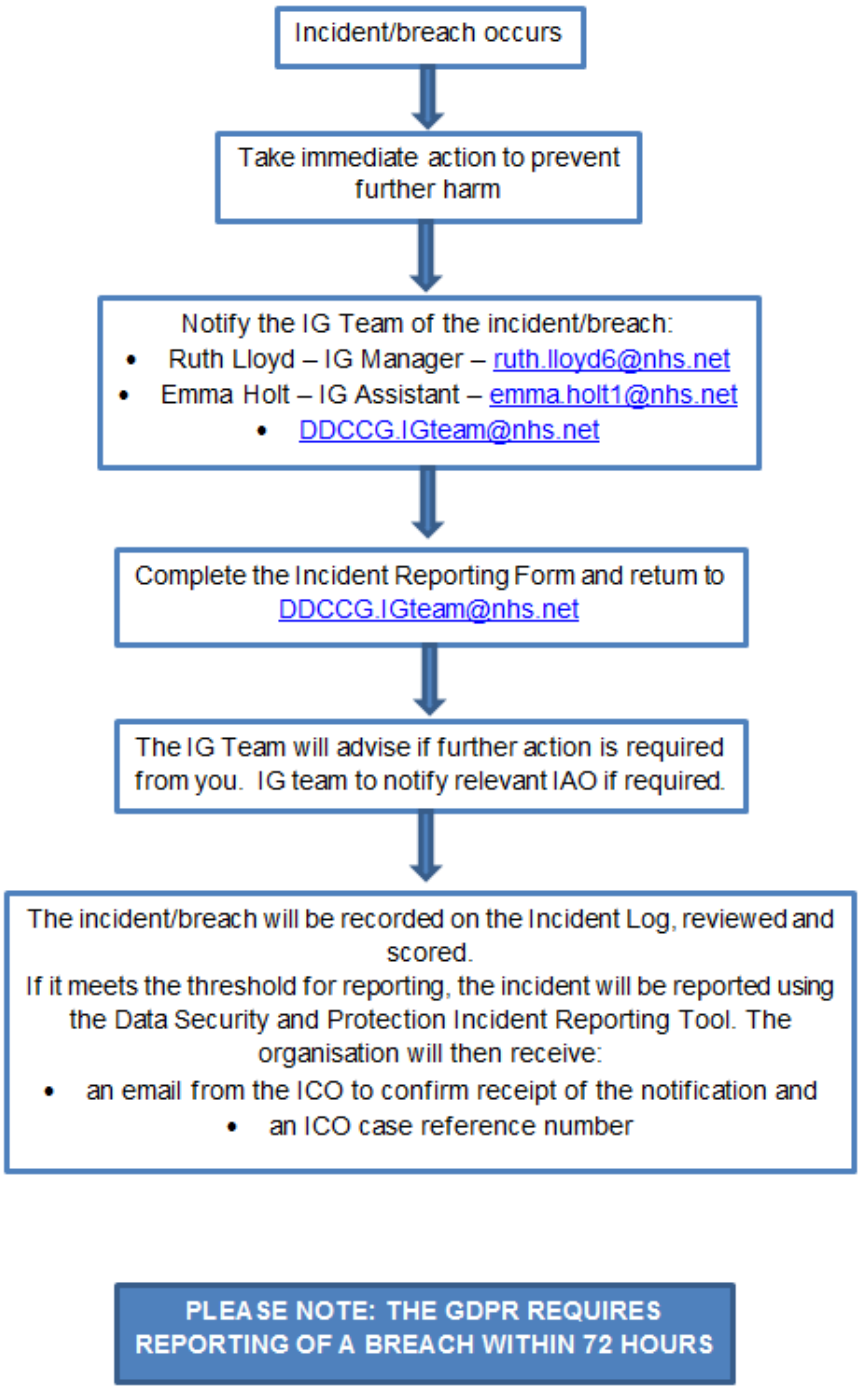


Appendix 2 – Information Governance Reporting Structure

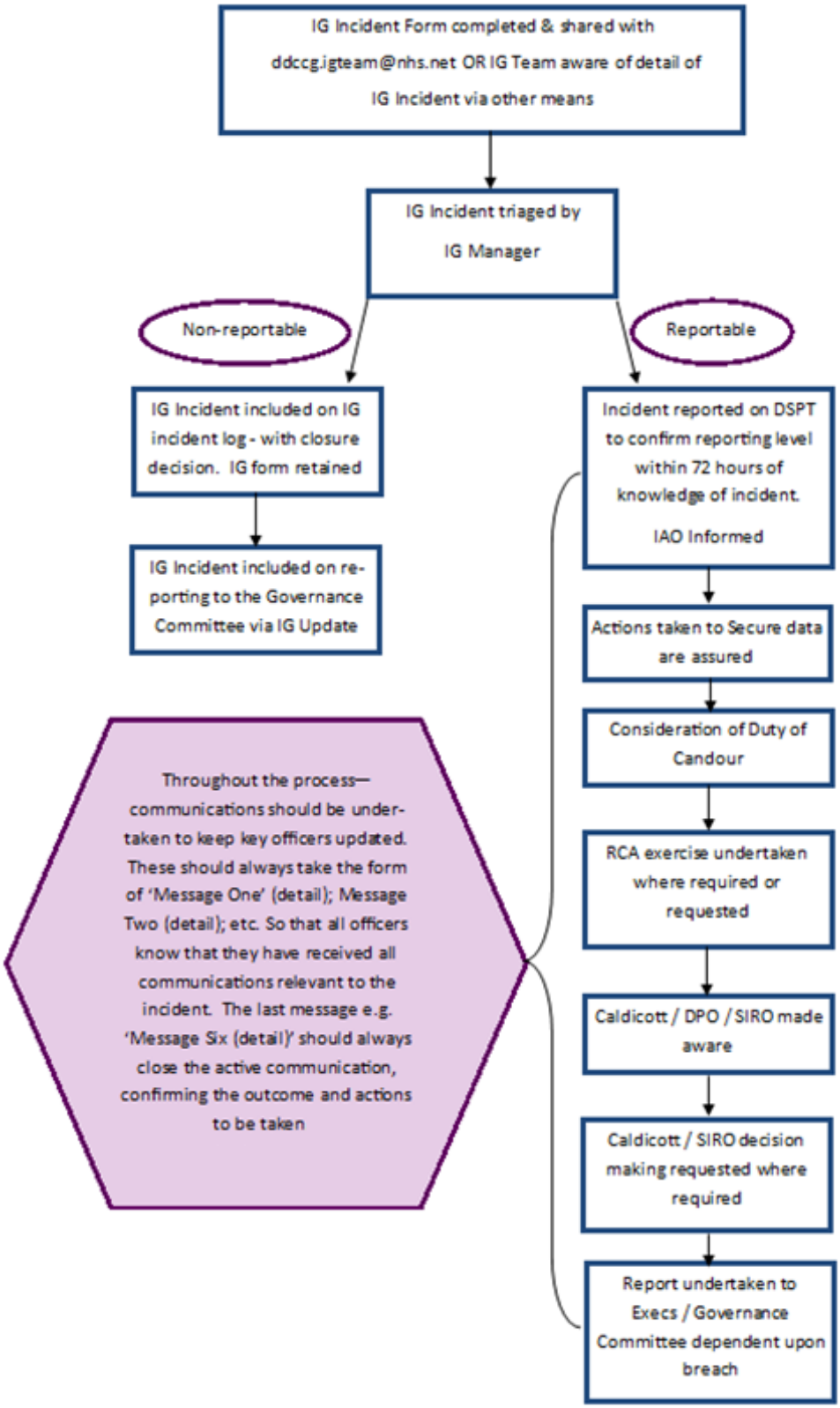


Appendix 3A – Information Governance Reporting Process Flow Diagram

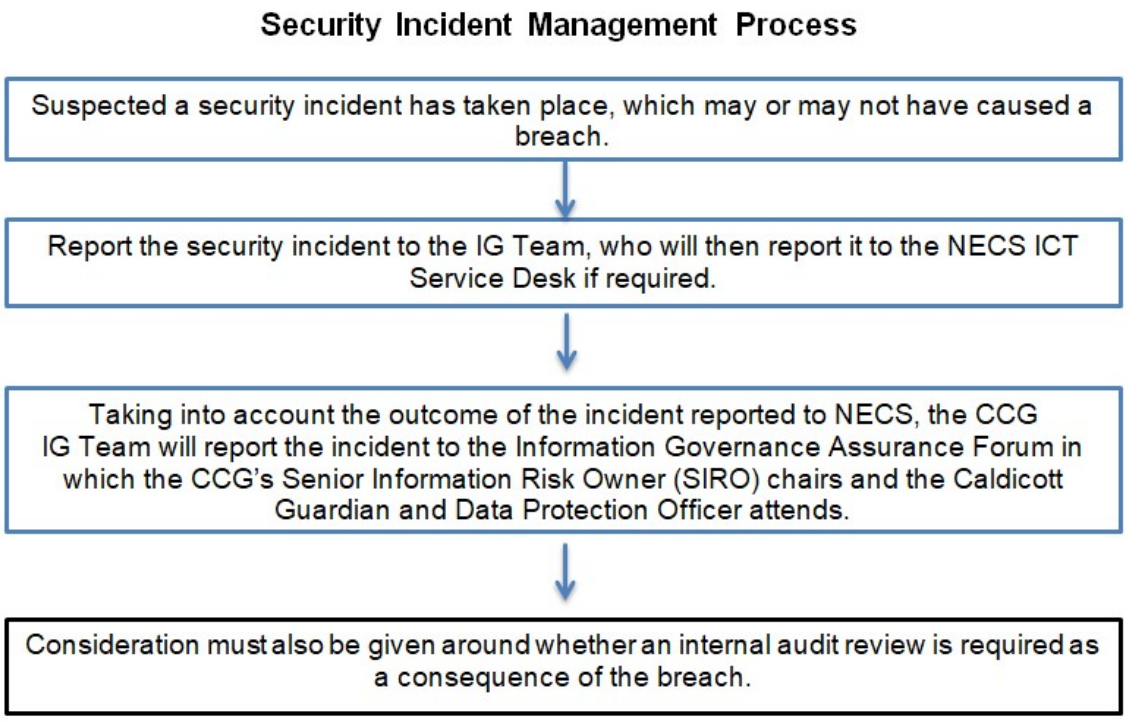
Incident Reporting Process Flow Diagram



Appendix 3B – Information Governance Incident Response Plan



Appendix 3C – Information Security Incident Management Process



Appendix 4 – Training Needs Analysis

Job Role	Data Security Awareness Level 1	The Caldicott Guardian in the NHS & Social Care	NHS Introduction to Risk Management for SIROs & IAOs	Information Asset Owner Training	Access to Health Records	Records Management
Frequency	Annually	Annually	Annually	One off session	Every 3 years	Every 3 years
IG Lead (CCG)	Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
Caldicott Guardian	Mandatory	Mandatory	Mandatory	Optional	Mandatory	Optional
SIRO	Mandatory	Optional	Mandatory	Mandatory	Optional	Optional
IAO & IAA	Mandatory	Optional	Mandatory	Mandatory	Optional	Optional
Data Protection Officer	Mandatory	Optional	Optional	Optional	Mandatory	Optional
Admin/Clerical	Mandatory	Optional	Optional	Optional	Optional	Optional
Admin/ clerical with access to personal information	Mandatory	Optional	Mandatory	Optional	Optional	Optional

Appendix 5 – Terminology

Term	Acronym	Definition
Anti-virus		Anti-virus software is used to prevent, detect, and remove malware, including computer viruses, worms, and Trojan horses.
Asset Register		A list of property owned by the organisation.
Audit		An official inspection, or evaluation, e.g. that the organisation's processes are being complied with.
Authentication		Ensuring that the identity of a subject or resource is the one claimed.
Availability		Ensuring that information is accessible and usable upon demand by authorised users.
Business Continuity		Strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level.
Business Continuity Management	BCM	Holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Management Lifecycle		Series of business continuity activities which collectively cover all aspects and phases of the business continuity management programme.
Business Continuity Management Programme		Ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review.
Business Continuity Plan	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable defined level.
Business Continuity Strategy		Approach by an organisation that will ensure its recovery and continuity in the face of disaster or other major incident or business disruption.

Term	Acronym	Definition
Business Data / Corporate Data		Data entered by users into an organisation asset, such as personal data or other files created by users.
Business Impact Analysis		Process of analysing business functions and the effect that a business disruption might have upon them.
Caldicott Guardian		A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing. Caldicott Guardians were mandated for NHS organisations by Health Service Circular HSC 1999/012 and later for social care by Local Authority Circular LAC 2002/2. General practices are required by regulations to have a confidentiality lead.
Caldicott Principles	Caldicott	The principles devised by the Caldicott Committee, which represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered.
Care Service		Delivery of health and social care needs and treatment to service users by or on behalf of health and social care organisations. Care services encompasses the use of personal information to provide: health and social care services directly to the individual; equipment services directly to the individual by a third party on behalf of, or in partnership with health or social care organisations; support services to health and social care organisations by a third party.
Clinical Spine Application	CSA	The web-based application that enables healthcare professionals who have access to local NHS Care Records Service systems and services to have controlled access to the national Personal Demographics Service and the Personal Spine Information Service.
Code of Conduct		A set of rules to guide behaviour and decisions in a specified situation.
Common Law		The law derived from decisions of the courts and case law, rather than Acts of Parliament or other legislation.
Computer Misuse Act 1990	CMA 1990	An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.
Confidentiality		Ensuring that information is not made available or disclosed to unauthorised individuals, entities or processes.
Confidentiality Breaches		When information has been given in confidence and is either disclosed to or accessed by an unauthorised person.

Term	Acronym	Definition
Confidentiality: NHS Code of Practice		A guide for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.
Data Controller		A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processor		In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Protection Act 2018		The Act of Parliament which regulates of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.
Data Security and Protection Toolkit	DSPT	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.
Denial of Service	DoS	Result of any action or series of actions that prevents any part of an information system from functioning.
Disclosure Log		A register containing information about ad hoc disclosures of personal information, useful for ensuring there is consistency in responding to disclosure requests.
Duty of Confidence		A duty of confidence arises when one person discloses information to another (eg patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a legal obligation that is derived from case law.
Electronic Health Record	EHR	An electronic record of the health and care provided to an individual.
Electronic Prescription Service	EPS	A service designed to reduce the paper administration associated with prescribing and dispensing processes by enabling prescriptions to be generated, transmitted and received electronically.
Encryption		The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Term	Acronym	Definition
European Economic Area	EEA	In the field of data protection, the EEA Agreement covers EU legislation of general application to commercial activities, such as the General Data Protection Regulation (EU) 2016/679 and all related "adequacy decisions" allowing international transfers of personal data with counterparties located outside the EEA, as well as the e-Privacy Directive 2002/58/EC and related acts such as Regulation (EU) No 611/2013 on notifications of data breaches.
European Union	EU	The European Union (EU) is an economic and political partnership between 27 democratic European countries. EU countries set up bodies to run the EU and adopt its legislation. The main bodies are the European Parliament (representing the people of Europe); the Council of the European Union (representing national governments); and the European Commission (representing the common EU interest).
Fair Processing		Processing broadly means collecting, using, disclosing, retaining or disposing of personal data. If any aspect of processing is unfair, there will be a breach of the first data protection principle – even if it can be shown that one or more of the conditions for processing have been met.
Freedom of Information Act 2000	FOIA 2000	The Act that makes provision for the disclosure of information held by public authorities or by persons providing services for them.
General Data Protection Regulations	GDPR	The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018. The UK adopted the principles of the GDPR by the enactment of the Data Protection Act 2018.
Human Rights Act 1998	HRA 1998	The Act which brought the rights and freedoms guaranteed under the European Convention on Human Rights into UK law.
Incident Reporting		A method or means of documenting any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or that is not in accordance with established policies, procedures or practices.
Information Asset		Operating systems, infrastructure, business applications, off-the-shelf products, services, user developed applications, documents, records and information.

Term	Acronym	Definition
Information Asset Administrator	IAA	Information Asset Administrators are usually operational members of staff who understand and are familiar with information risks in their area or department, e.g. Security Managers, Records Managers, Data Protection Officers, Internal Audit. For smaller organisations, an appropriate operational role may include Office or Departmental Managers, Shift Supervisors and senior administrative staff. Information Asset Administrators will implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.
Information Commissioner's Office	ICO	The United Kingdom's independent public body (UK Supervisory Authority) set up to uphold information rights in the public interest and data privacy for individuals.
Information Governance	IG	A term used in the NHS for the principles, processes, legal and ethical responsibilities for managing and handling information. Information governance (IG) sets the requirements and standards that the NHS must achieve to ensure it fulfills its obligations to handle the information securely, efficiently and effectively.
Information Governance Framework		The information governance framework for health and social care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that the set standards are clearly defined and met. Whilst a key focus of information governance is the use of information about service users, it applies to information and information processing in its broadest sense and underpins both clinical and corporate governance.
Information Governance Lead		IG Lead A senior representative in the organisation who leads and co-ordinates the information governance works programme.

Term	Acronym	Definition
IG Security Accreditation Documentation		The records kept of all security controls applied to a particular information asset, including assessments and reviews of those controls
Information Governance Statement of Compliance		IG SoC An agreement between NHS Digital and any organisation wishing to use services provided through the spine. The agreement stipulates the obligations which the organisation is expected to maintain to ensure patient data is safeguarded and only used appropriately.
Information Lifecycle Management		ILM Refers to the management of information throughout its lifecycle; from the point of its creation through to its eventual disposal
Information Risk Lead		The person assigned lead responsibility for the identification, assessment and control of risk to business information and information systems.
Information Security		Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.
Information Security Event		An identified occurrence of a system, service or network state indicating a possible breach, or a previously unknown situation which may be security relevant of information security policy or failure of safeguards.
Information Security Management: NHS Code of Practice		A guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England.
Information Standards Board ISB		The Information Standards Board (ISB) approves information standards used in the NHS (England) and in its work with other agencies such as social care.
Information Standards Notice ISN		Previously known as Data Set Change Notices, Information Standards Notices are the formal notifications through which new, and changes to existing, information standards are announced.
Integrity		Ensuring the accuracy and completeness of assets.

Term	Acronym	Definition
Key IT Equipment		IT equipment that is necessary for delivering NHS or Social Care services. It encompasses the categories defined as key electronic systems and key operational systems, but also includes peripheral equipment without which these key systems could not function
Key Operational System		These are the key operational systems for collecting and holding patient or service user information. In hospitals, the Patient Administration System (PAS) is often the main database for most data used, but other, department, systems (e.g. Pathology, Radiology, A&E systems) which are used for the operational delivery and organisation of care may also need to be included. In primary care, the key system may be the General Practice System. For Social Care organisations, this may be the Social Care Electronic Record System.
Legitimate Relationship		Staff involved in an individual patient's care are considered to have a 'legitimate relationship' with that patient. Access to confidential information about each patient is limited to those staff who have a 'legitimate relationship' with that patient.
Local Service Provider		Local Service Providers are responsible for delivering services at a local level and supporting local organisations in delivering the benefits from them. They ensure the integration of existing local systems and, where necessary, implement new systems to ensure that the national applications can be delivered locally, while maintaining common standards.
Malicious Code		Software that interferes with the normal operation of a computer system and executes without the express consent of the user. Malicious code includes programs such as viruses, worms and Trojans that can perform unauthorised processes on a computer or network such as sending an email, stealing passwords or deleting information.
Malware		Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.
Mental Capacity Act 2005		MCA 2005 An Act of Parliament which made new provisions relating to persons who lack mental capacity to make decisions for themselves.
Network Sniffing		A network sniffer is a program or device that monitors data travelling over a network.
Networked Data		Data which is stored and can be accessed by computerised systems linked to the same network.
NHS Care Records Service	NHS CRS	The NHS Care Records Service is a secure service that links patient information from different parts of the NHS electronically, so that authorised NHS staff and patients have the information they need to make care decisions. There are two elements to the NHS Care Records Service: detailed records (held locally) and Summary Care Records (held nationally).

Term	Acronym	Definition
NHS Resolution		NHS Resolution handles negligence claims and works to improve risk management practices in the NHS. They are also responsible for resolving disputes between practitioners and primary care trusts, giving advice to the NHS on human rights case law and handling equal pay claims on behalf of the NHS.
NHS Network N3 – moving to the Health and Social Care Network HSCN	N3 / HSCN	NHS Network is the high speed private broadband computer network used by the NHS and its partners.
NHS Number		A national number assigned to all patients registered with the NHS in England and which is used by the NHS and social care as a unique patient identifier.
NHS Operating Framework		Issued normally in December each year, the NHS Operating Framework sets out the Department of Health's specific business, financial arrangements and priorities for the NHS for the following financial year.
NHSmail		NHSmail is a secure national email and directory service used to transmit email messages between NHS organisations.
Non-Care Purpose		The use of information for a purpose that does not directly contribute to the diagnosis, care and treatment of an individual, or to the audit/assurance of the care provided.
Non-Disclosure Clause		Is a clause within a contract that requires that the parties to the contract do not share the material, knowledge or information pertaining to the contract with anyone that is not a party to the contract.
Patient Identifiable Information		Any information that may be used to identify a patient directly or indirectly. Key identifiable information includes patient name, address, date of birth, full post code, images, tapes, NHS number and local identifiable codes.
Penetration Test		A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source.
Person Identifiable Information		Information about a person which would enable that person's identity to be established. This might be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Term	Acronym	Definition
Personal Data		Any information which fall within the remit of the UK Data Protection Act 2018. Also referred to as Person Identifiable Data (as defined within the DPA 2018).
Personal Demographics Service		PDS The national electronic database of basic NHS patient demographic details and their NHS Number. It enables a patient to be readily identified by healthcare professionals, and associated with their medical details.
Policy		A policy is a statement of an organisation's intentions and approach to fulfilling its statutory and organisational responsibilities. Policies are underpinned by relevant evidence and guidelines and enable management and staff to make correct decisions, work effectively and comply with relevant legislation and an organisation's aims and objectives. They may be supported by relevant procedures.
Portable Devices		Refers to devices which are handheld or worn; for example, laptops, personal digital assistants, smart phones.
Position Based Access Control	PBAC	PBAC defines access control requirements by job role allowing for any number of employees to share generic access rights based on what they do rather than who they are. Referred to also as Role Based Access Control – RBAC.
Procedure		A procedure is a set of detailed step-by-step instructions that describe the appropriate method for carrying out tasks or activities to achieve a stated outcome to the highest standards possible and to ensure efficiency, consistency and safety.
Process		A process is the practical workings of one or more procedures that are linked in order to meet a policy requirement.
Public Records Act 1958	PRA	An Act to make new provision with respect to public records and the Public Record Office, and for connected purposes. It includes duties about selection and preservation of public records, places of deposit, access and destruction.
Publication Scheme		A publication scheme sets out the kinds of information that a public authority should make routinely available. The information should be easy for the authority and any individual to find and use. This is a requirement of the Freedom of Information Act (FOIA) (2000).
Records Management		Records management is the practice of maintaining the records of an organisation from the time they are created up to their eventual disposal. This may include naming, version control, storing, tracking, securing, and destruction (or in some cases, archival preservation) of records.

Term	Acronym	Definition
Records Management: NHS Code of Practice		A guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on legal requirements and professional best practice.
Registration Authority	RA	RA Manages the registration and access control processes required to ensure that individuals who need to access the NHS Care Records Service and related IT services have had their identity rigorously checked and are assigned appropriate access. All spine based national NHS systems require smartcard access prior to access being granted.
Registration Authority Agent	RAA	Responsible for ensuring Registration Authority services are delivered to users in accordance with policy and governance, including registration of sponsors and healthcare professionals.
Registration Authority Manager	RAM	RAM Responsible for ensuring that Registration Authority services are provided in accordance with policy and procedure requirements identified by the Department of Health / NHS Digital, and for the efficient day to day operation and capacity planning of the services.
Registration Authority Sponsor	RAS	Responsible for approving, where appropriate, the registration and profiles to be granted to users. Additionally, they may be responsible for the appropriate issue of Fall back (temporary use) Smartcards, Passcode resetting and vouching for the identity of users – all subject to the policy and governance framework.
Risk		Something that might happen and its effect(s) on the achievement of objectives.
Risk Appetite		Total amount of risk that an organisation is prepared to accept, tolerate or be exposed to at any point in time.
Risk Management		Structured development and application of management culture, policy, procedures and practices to the tasks of identifying, analysing, evaluating, and controlling responding to risk.
Role-Based Access Control	RBAC	Grants a view of a patient's record depending on the role the individual was assigned when they registered for access to the NHS Care Records Service and related IT services. Authorised users are only able to access the information they need to carry out their role, e.g. a booking clerk will see less information than a doctor.
Safe Haven		A location (or system) within an organisation where arrangements and procedures are in place to ensure personal information can be held, received and communicated securely.

Term	Acronym	Definition
Secondary Uses Service	SUS	The Secondary Uses Service is the single source of comprehensive data to enable a range of reporting and analysis. SUS supports the NHS and its partners in the areas of planning, commissioning, management, research, audit, public health and a number of national initiatives.
Section 251		This relates to section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001). It allows the common law duty of confidentiality to be set aside in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable. Applications for approval to use Section 251 support are considered by the Ethics and Confidentiality Committee of the Confidentiality Advisory Group.
Senior Information Risk Owner	SIRO	An Executive Director or member of the Senior Management Board with overall responsibility for the organisation's information risk policy. The SIRO will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.
Serious Incident Requiring Investigation	SIRI	Any IG incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals is regarded as serious. The severity of the incident determines the action to be taken following the incident.
Service User		A person who receives or is registered to receive attention, care, or treatment. The term includes patient, clients and other users of the service provided by the organisation
Smartcard		A card similar to a chip and PIN credit or debit card, but more secure. A Smartcard controls who has access to a particular computer system and what level of access they can have. An NHS Care Records Service user's Smartcard is printed with their name, photograph and unique user identity number.
Strategy / Strategies		A strategy is a plan designed to achieve a particular long-term aim. Strategies usually cover 3-5 years and are designed to achieve particular goals or objectives. A strategy is often a broad statement of an approach to accomplishing these desired goals or objectives, and can be supported by policies and procedures.
Teleworking		A form of organising and/or performing work, using information technology, in the context of an employment contract/relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis.
Terms of Reference	ToR	Describes the purpose and structure of a project, committee, meeting, negotiation, etc.

Term	Acronym	Definition
Third Sector Organisation		An organisation that occupies the space between the state and the private sector. These include small local community and voluntary groups, registered charities (both large and small), foundations and trusts, as well as social enterprises and co-operatives.
Trojan		Non-self-replicating malware that appears to perform a desirable function for the user but instead enables unauthorised access to the user's computer system.
Trusted Organisation		An organisation that has completed the Data Security and Protection Toolkit (previously the Information Governance Toolkit) is registered as a “trusted organisation”. Note: the organisation may have an action/improvement plan in place to improve its attainment levels.
Vicarious Liability		An employer is vicariously liable for negligent acts or omissions by his employee in the course of employment, whether or not such act or omission was specifically authorised by the employer. To avoid vicarious liability, an employer must demonstrate either that the employee was not negligent in that the employee was reasonably careful or that the employee was acting in his own right rather than on the employer's business.
Virus		A computer program that can copy itself and infect a computer.
Voice Over Internet Protocol	VOIP	A general term for a family of transmission technologies for delivery of voice communications over Internet Protocol networks.
Worm		A self-replicating malware computer program. It uses a computer network to send copies of itself to other computers on the network and can do so without any user intervention.

Appendix 6 – Governing Body Responsibilities for Information Governance

Guidance for NHS Boards: Information Governance

Information governance aims to support the delivery of high quality care by promoting the effective and appropriate use of information. The Information Governance framework for Health and Social Care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that these standards are clearly defined and met. Whilst a key focus of information governance is the use of information about service users, it applies to information and information processing in its broadest sense and underpins both clinical and corporate governance.

The NHS Chief Executive, in his communications to NHS Chief Executives, has made it clear that the ultimate responsibility for information governance in the NHS rests with the Board of each organisation. Boards should note that:

- Information governance should be explicitly referenced within each organisation's statement of internal controls.
- An effectively supported Board level Senior Information Risk Owner (SIRO) is required in each organisation and should update the Board regularly on information risk issues.
- Appropriate annual information governance training1 is mandatory for all staff who have access to personal data and for all those in key roles.
- An annual information governance assessment (the Data Security And Protection Toolkit (DSPT)) must be undertaken with performance assessments published for review by the regulatory bodies3.
- Details of serious untoward incidents involving actual or potential loss of personal data or breach of confidentiality must be published in annual reports and reported in line with Department of Health guidelines, including to the Information Commissioner.

NHS Board members need to ask themselves:

1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures and are addressing the responsibilities and key actions required to support effective Information Governance?"
Governance Committee is delegated by the Governing Body to have oversight of the delivery of the IG agenda. The IG Assurance Forum, Chaired by the CCG SIRO is established and ensures the delivery of the IG strategy and work plan. The Data Security and Protection Toolkit delivery is overseen here, alongside reporting of Incidents, Subject Access Requests, Caldicott Issues, Mandatory Training, Policy development and staff engagement.
2. "What were the outcomes of our most recent annual Information Governance assessment, and what measures (if any) have been put in place to address any identified deficiencies?"
The DSPT for 2019/20 was assessed by 360 Assurance as a 'substantial assurance' audit outcome.
3. "What plans do we have in place to ensure our organisation remains compliant with national standards for Information Governance?
During March 2020, the Governance committee received the 2020/2021 work plan for Information Governance which aims to build on the foundations of the 2019/20 financial year.
4. "Do we as an organisation have the capacity and capability to guarantee our plans for Information Governance can be implemented?"
The recent Cyber Operational Readiness Support (CORS) work identified a 'strong and engaged IG manager', supported by active executive support as Caldicott Guardian, SIRO and Data Protection Officer.
5. "Do our information governance arrangements adequately encompass all teams and work areas that we are legally accountable for?"
The role of IG for the CCG is in place, and is assured. GP practice IG support is provided via NECS, although visibility of their activity and reporting is not currently in place. IG support for organisations with whom the CCG has contracted (not GP) is not in place, and the role of contracted organisations as data controllers is affirmed at contract commencement. The CCG is not assured presently that each contracted organisation is compliant with the DSPT, and this is part of ongoing contract management works.