NHS
Waltham Forest
Clinical Commissioning Group

NHS Waltham Forest
Clinical Commissioning Group
Information Governance Policy

Author:	Zeb Alam, CCG IG Lead, (NELCSU) David Pearce, Head of Governance, WFCCG
Version	3.0
Amendments to Version 2.1	Annual review and update: Reference to Caldicott Guardian plan and assurance with the Caldicott review Reference to Public Interest Disclosure Act on protected disclosures and Public Information Policy to be reviewed every 2 years unless national changes or changes in legislation warrant an earlier review
Amendments to Version 3.0	Addition of Data Protection Officer role Amendment to references to Data Protection Act 1998 Amendment from references to IG Toolkit to Data Protection and Security Toolkit
Review date:	March 2019

Contents

Summary

Waltham Forest Clinical Commissioning Group (CCG) has put this policy in place to ensure staff are fully aware of their Information Governance (IG) responsibilities. This policy is important as it should help you understand how to look effectively manage and best utilise the information needed to do your jobs consistent with the law and expected standards.

Information is a valuable asset to a commissioning organisation to enable it to effectively make informed decisions. Therefore it is important to ensure we maximise the value of information as an 'asset' in compliance with legal requirements. To do this we will ensure information is:

- **H**eld securely and confidentially;
- **O**btained fairly and lawfully;
- **R**ecorded accurately and reliably;
- **U**sed effectively and ethically; and
- **S**hared and disclosed appropriately and lawfully.

The CCG is committed to ensuring that information, in whatever its context, is processed as determined by prevailing law, statute and best practice including the Caldicott2 Report 2013 and its recommendations. Compliance with all organisation policies is a condition of employment and a breach of policy may result in disciplinary action.

1. Scope

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

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

2. Introduction

Information Governance is a framework to manage information appropriately. It ensures confidentiality and security, as well as that processes are in place to ensure appropriate standards of quality and ethical use of personal information. Corporate information and records must also be managed appropriately, and where possible and appropriate provided to the public to ensure transparency and accountability.

The CCG uses information to support the commissioning and management of commissioning of patient healthcare. Information is also used to support the administration of the NHS and wider Health economy. In addition to these functions are the duties of the Clinical Commissioning Group as detailed in statute.

The NHS and the administration of the NHS depends on the appropriate use of Personal Data and management of secondary use of this data.

As a commissioner of services we require good quality information to be created, managed and utilised by those we commission. The organisation is responsible for driving improvements in IG from

these services. This ensures an efficient, effective and accountable service. In those instances where we appropriately share or publish information we must ensure that this done in a lawful and appropriate manner.

Information is transferred to other organisations and the suppliers of services to support these functions and disclosed in accordance with statutory, regulatory or organisational requirements.

Good quality Information forms a key component of the NHS Information Revolution with the aim of giving people more control over their own care. This restates the NHS's intention to promote effective decision making and ensure patients are informed and empowered through provision of information that is accurate, accessible and coherent.

This organisation must discharge its statutory and organisational responsibilities. All staff, and those working on our behalf, are responsible and contribute towards effective and responsible governance of information in line with the organisation's aims and objectives.

This policy provides an overview of how information will be governed and used in the CCG; it also outlines how the organisation will discharge it duties. This requires a systematic and consistent approach based on controls owned, understood and supported by all those working on its behalf.

3. Purpose

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

Confidentiality

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

Integrity

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

Availability

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

Accountability

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

Roles and responsibilities

The CCG has identified the following relevant roles and responsibilities within the organisation.

Role	Responsibilities
Governing Body	In line with the Guidance for NHS Boards: Information Governance, the governing body will ensure that its organisation has taken appropriate steps to meet IG standards. In particular it will seek assurance against following questions: 1. "What have we done, as an organisation, to ensure we have implemented adequate policies and procedures, and are addressing the responsibilities and key actions required to support effective IG?" 2. "What were the outcomes of our most recent annual IG assessment, and what measures (if any) have been put in place to address any identified deficiencies?" 3. "What plans do we have in place to ensure our organisation remains compliant with national standards for IG? 4. "Do we as an organisation have the capacity and capability to guarantee our plans for IG can be implemented?" 5. "Do our IG arrangements adequately encompass all teams and work areas that we are legally accountable for?" 6. What plans do we have in place to ensure commitment to the Caldicott 2 recommendations in relation to strengthening our process for managing patients dissent to use of their information? 7. How would we manage FOI request on disclosure of Information as a result the Public Information Regulations?
Accountable Officer	Has overall accountability and responsibility for governance within the organisation. Is to provide assurance that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the IG agenda. • Fosters a culture for protecting and using data. • Ensures information risk requirements are included in the corporate Risk and Issue Management Policy. • Ensures Information Asset Owners (IAOs) undertake risk assessments of their assets. • Is responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Provides a focal point for the management, resolution and/or discussion of information risk issues. • Ensures that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff. • Ensures the Governing Body is adequately briefed on information risk issues. • Is accountable for information risk. The SIRO roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance. The role holder will be supported and advised by the IG Team.

Role	Responsibilities
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues. Ensure that the CCG completes all requirements in the Caldicott work plan relevant to the CCG. These requirements are further linked into the annual IG work plan. The Caldicott Guardian is supported in this role by the IG Lead and the IG Team who provide the Caldicott Function for the organisation. There are delegated roles and responsibilities and other delegated roles within the CCG and CSU to support delivery of the Caldicott Work Plan and assist with the completion of the Caldicott plan for the organisation. The Caldicott Guardian is required to maintain an Issue log.
Data Protection Officer	The Data Protection Officer (DPO) reports to the SIRO and the highest level of management. This ensures the DPO can act independently and without a conflict of interest. The DPO is responsible for ensuring that the CCG and its constituent business areas remain compliant at all times with Data Protection Act 2018, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations (information rights legislation). The DPO shall: lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards. Provide a central point of contact for the information rights legislation both internally and with external stakeholders (including the office of the Information Commissioner). The CCG must ensure that the DPO is consulted on: • whether or not to carry out a Data Protection Impact Assessment (DPIA) and the DPIA methodology; • what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; • whether or not the data protection impact assessment has been correctly carried out and whether its conclusions are in compliance with the GDPR; and • data breaches

Role	Responsibilities
Information Security Officer	This role will be fulfilled by the North and East London CSU IG Team, IT team and local facilities management depending on the requirement. Provides advice to information owners on potential information risks and controls. Support in any risk reviews with departments.
Information Asset Owners	All senior staff at Director level are required to act as Information Asset Owners for the information assets within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assists identified as within their remit. They will also: • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. The IAOs will be supported by IAAs who will ensure the above takes place. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance.
Information Asset Administrators	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how they work and how they are used. They will ensure there are procedures for using them, control access to them and understand their limitations. The detailed roles and responsibilities are defined in Appendix A of the NHS Information Risk Management Guidance.
IG Lead	Senior CCG Manager responsible for ensuring suitable advice, guidance support, tools and training are available to those with the CCG who handle data, to ensure they do so appropriately. This role will be the main point of contact for the NEL CSU IG Team.
NEL CSU IG Team	Provide specialist advice and support, under contract, to the organisation in relation to IG subject matters. They will also form part of the Caldicott function and associated plan.
All Substantive/ Permanent Staff	All those working for the CCG have legal obligations, under the Data Protection Act and common law of confidentiality; and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct to manage information appropriately. These are in addition to their contractual obligations which include adherence to policy, and confidentiality clauses in their contract.
Third parties	The same responsibilities as for permanent staff apply to those working on behalf of the organisation, whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of, but not directly employed by, the organisation are required to sign a third party agreement outlining their duties and obligations.

Role	Responsibilities
CCG Member Practices	This policy should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its functions. However it is recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.

4. Policy Standards

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

4.1. Accountability and Governance

The CCG will put in place suitable controls to:

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

4.2. Managing Information Risk

The CCG will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes. A failure to effectively implement information could lead to the following risks.

Risk	Example
Reputational Damage	• Making decisions from inaccurate information could undermine any commissioning decision could affect organisational reputation.
Financial Loss	• Loss of information could lead to financial penalties of up to £500,000 • Inefficient use of information may lead to duplication and wasted time.

Failure to comply with legal, regulatory or NHS requirements	• There are a number of lawful requirements to manage information such as the Data Protection Act, Freedom of Information Act, Public Records Act and Caldicott Principles which could also lead to reputation or financial loss • Failure to be compliant with NHS Constitution or NHS Care Records Guarantee or CCG Authorisation requirements.

4.3. Openness and Transparency

The CCG will put in place systems and processes to ensure, where appropriate, unrestricted information is made available to the public. Individuals should be aware of how to access this and their own information:

- Suitable processes will be put in place to meet requirements of the Freedom of Information Act 2000 and NHS Code of Openness including
- Staff will be made aware of the need to use protective markings such as NHS Official or Restrict as defined within the Information Security Policy and Appendix D.
- Individuals will be made aware of how their information will be processed using privacy notices, unless legally exempt from the requirement
- Requests for access to personal data will be managed in line with legal requirements and best practice
- Information, including personal and sensitive data, will be shared with other agencies only where there is a legal basis to do so and to comply with the Caldicott 2 recommendations

4.4. Use of information

Information is used, processed, or created by the organisation for the pursuit of its legitimate business interests and discharge of its statutory functions. All use of information within the organisation and by those working on its behalf must be in accordance with these objectives and obligations.

All information must be used, created and managed in a professional and business-like manner. It must be accessible to the organisation on a long term basis and must be stored in a systematic and consistent manner.

Access to information systems, such as email, databases, the internet or network, and records of the organisation are provided to staff for business purposes. All access and use must be appropriate and in line with the discharge of their duties.

As staff create information they are doing so on behalf of the organisation, for example when sending emails, and are accountable for the appropriateness and accessibility of information they create.

4.5. Personal Confidential Data

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

Information provided to the NHS is done so on the expectation of confidence and often in a healthcare setting. It is important for staff and working practice to account for this and to ensure that any

secondary use of personal data, for non-care purposes, is carried out in accordance with legal, regulatory and organisational requirements.

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

Each directorate within the Organisation should provide a clear statement for their area of its responsibility where they process Personal Confidential Data.

A definition of Personal Confidential Data is provided in Annexe B.

4.6. Use of Information to improve performance

The CCG will actively seek opportunities to improve its performance and the performance of those organisations it commissions by the better use of information and data. This includes:

- Use of pseudonymised, anonymised or de-identified patient data to inform better health care decisions for individuals and the community;
- To review processes and functions within the organisation to ensure efficient and effective data processing;
- To support appropriate information sharing initiatives and ensure that the patient and public can exercise choice about the use of their data as well as ensuring they are kept informed about proposed uses including the sharing of their information.

Any change processes within the organisation are required to account for the requirements to ensure appropriate and effective information management. All staff managing change must ensure that they scope potential IG issues before commencing the change process.

4.7. Information Security

The CCG will put in place systems and processes to maintain the security of information where it is required. This will include:

- Establishing and maintaining policies for the effective and secure management of information assets and resources.
- Undertaking or commissioning annual assessments and audits of its information and IT security arrangements.
- Promoting effective confidentiality and security practice to its staff through policies, procedures and training. The training required by role is set out at Appendix E
- Having in place secure mechanisms for the exchange of information in a variety of forms, including but not limited to secure post, email, encrypted storage media etc.
- Encouraging safe and secure utilisation of IT services and products to meet efficiency demands whilst still maintaining the suitable availability, confidentiality and integrity of the data at all times
- Establishing and maintaining incident reporting procedures and monitoring and investigating all reported instances of actual or potential breaches of confidentiality and security. Such incidents will be managed in accordance with the Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation.

- Undertaking information risk assessment, in conjunction with overall priority planning of organisational activity to determine appropriate, effective and affordable IG controls are in place in relation to the acquisition, transfer and storage of data
- Where information risks are assessed these will be considered in line with the international information security standards ISO 27001 and ISO 27005

Further information can be found in the Information Security Policy.

4.8. Information / Records Management

Information is the key resource of the National Health Service (NHS) and the wider health economy, it enables the effective treatment of patients and the management of the NHS system and the services we commission. Information Management requires the management of information from creation and use all the way through to destruction or archival retention.

Appropriate management of information enables an organisation to reduce costs, improve efficiency and enhance the ability to monitor the performance of contracts and commissioned services. Understanding the information we hold and the way our organisation uses it helps us to manage our responsibilities under legislation, such as the Data Protection Act.

The CCG will ensure that information management principles, controls and standards are in place for each stage of the information's lifecycle. Staff are responsible for maintaining these controls and standards.

In order to support effective commissioning and to support efficiency, all systems and standard working practice involved in the processing of information must ensure the accuracy and quality of information. The Policy on Information Quality provides more details.

4.9. Information Quality:

The CCG recognise the importance of quality information to make informed decisions. As such the CCG will ensure processes are in place to maintain:

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

Further details can be found in the Policy on Information Management.

5. Training

All staff are, as a minimum, mandated to undertake the “Introduction to Information Governance” e-learning module once followed by the “Information Governance Refresher” on an annual basis. Additional training needs analysis will be undertaken periodically and staff should comply with any recommendations identified. There are specific e-learning training requirements specified in Appendix E by roles for the Senior Information Risk Owner (SIRO), Caldicott Guardian and Information Asset Owners (IAOs) and Information Asset Administrators (IAAs)

6. Relationship with Service Providers

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

6.1. Clinical Services

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

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

6.2. Support services

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

- A suitable contract is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG
- The services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office
- Completion of the annual t Data Security and Protection Tookit and undertake an independent audit/service review, to be disclosed to the CCG on request in order to provide assurance they have met expected requirements.
- That any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity
- Report any known incidents or risks in relation to the use or management of information owned by the CCG

7. Equality and Diversity

As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with expected Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on

employees, patients and the public on the grounds of protected characteristics such as race, social exclusion, gender, disability, age, sexual orientation or religion/belief.

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

8. Dissemination and Implementation

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

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

9. Non-Conformance with this Policy

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

a. Accepted and reviewed in line with this policy

b. Accepted with a view to implementing an action plan to reduce the risk

c. Not accepted and the practice will stop until such time as the risk can be reduced

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

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958

10. Monitoring and Review

Performance against the policy will be monitored against

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

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

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

- identified deficiencies, risks or following significant incidents reported;
- changes to organisational infrastructure.

Appendices

Appendix A. Evaluation protocol

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

Appendix B. Equality Analysis

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

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

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

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

Appendix C. Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	The Information Governance Review, Mar 2013 (Gateway Ref: 2900774) page 125
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	

Appendix D: Privacy Markings

Marking	Description
Protective Marking	Records should be marked to signify the nature of the contents and the level of security that should be applied to them.
NHS Official	All routine CCG business, operations and services should be treated as OFFICIAL. The subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL should be used where applicable. Ordinarily NHS Official information does not need to be marked.
NHS Official-Sensitive	This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.
NHS Official-Sensitive: Commercial	Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the CCG, other NHS body or a commercial partner if improperly accessed.
NHS Official-Sensitive: Personal	Personal information relating to an identifiable individual where inappropriate access could have damaging consequences.

Appendix E: Training

Role(s)	IGTT Mandatory modules and HSCIC link	IGTT Recommended module and HSCIS link
Senior Information Risk Owner (SIRO)	NHS Information Risk Management for SIROs and IAOs Information Governance: The Refresher Module (if done intro to IG module previously) Business Continuity Management	Information Security Management Information Security Guidelines
Caldicott Guardian (CG)	The Caldicott Guardian in the NHS and Social Care Information Governance: The Refresher Module (if done intro to IG module previously) Patient Confidentiality	
Information Asset Owners (IAOs)	NHS Information Risk Management for SIROs and IAOs Information Governance: The Refresher Module (if done intro to IG module previously) Secure Transfers of Personal Data Business Continuity Management	Information Security Guidelines Password Management
Information Asset Administrators (IAAs)	Secure Transfers of Personal Data Password Management IG refresher (if done IG Introduction) Information Security Guidelines	Business Continuity Management
All staff who completed IG training last year	Information Governance: The Refresher Module	
New entrants and others who have not completed any IG Training	Introduction to Information Governance	
IG Lead	Information Governance: The Refresher Module (if done IG Intro first) Information Security Management NHS Information Risk Management for SIROs and IAOs Secure Transfers of Personal Data	Records Management and the NHS Code of Practice Business Continuity Management Password Management