

Information Governance Policy and Framework

Version No 2.6: February 2025

First Issued: October 2016
Review date: February 2028

Contents

(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)

- 1. INTRODUCTION 3
- 2. PURPOSE 4
- 3. SCOPE 4
- 4. DEFINITIONS 5
- 5. RESPONSIBILITIES 6
- 6. POLICY STATEMENT 7
- 7. PROCEDURE 7
- 8. MONITORING AND REVIEW 9
- 9. REFERENCES 9
- 10. ASSOCIATED POLICIES & PROCEDURES (To include but not limited to) 9
- 11. AUTHOR 10
- 12. APPENDICES 10
 - 1. *Appendix – Senior Information Governance Roles and Responsibilities* 11
 - 2. *Appendix – Equality & Diversity Impact Assessment* 11
 - 3. *Appendix – Documents Control Sheet* 12
 - 4. *Appendix – Version Control* 13
 - 5. *Appendix – IG Handbook* 14

1. INTRODUCTION

Information is a vital asset and plays a key part in clinical governance, corporate governance, and service planning and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

ECCH recognises the need for an appropriate balance between openness and confidentiality in the management and use of information, thus ensuring we can account for our actions as a Public Authority by routinely making certain information available to the public whilst equally preserving the confidentiality of personal information about individuals, and commercially sensitive information. ECCH also recognises the need to share identifiable personal information with other health organisations and agencies in a controlled manner consistent with the interests of the individual and, in some circumstances, in the public interest.

ECCH believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff members to ensure and promote the quality of information as this is often used in decision making processes.

ECCH have developed a framework for their Information Governance Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance. This policy acts as an overall umbrella policy sitting over the other policies relating to each aspect of Information Governance (IG), which provide more detail on the way in which the different initiatives are managed within the organisation. All of the other policies which fall into the various areas of IG; Confidentiality, Data Protection, Records Management etc., are traceable up to the IG Policy.

Policy	Description
Information Governance (IG) Handbook	The IG Handbook is a reference and guide to signpost Staff to the ECCH's Information Governance Policies & Procedures and explains IG at ECCH and the correct IG procedures.
Data Protection & Personal Information Handling Policy	The purpose the Data Protection & Personal Information Handling Policy is to provide employees and workers of ECCH with guidance as to the correct and lawful processing of information. Ensuring that all employees and workers of ECCH are aware of their legal and contractual obligations in terms of data protection.
Confidentiality Policy	The purpose of the Confidentiality Policy is to ensure the security and confidentiality of information relating to or held by the organisation. It is also policy to comply with all relevant legislation and regulation relating to the collection, storage, sharing and disposal of information
Data Protection & Impact Assessment Policy & Procedure	The purpose of the Data Protection & Impact Assessment Policy & Procedure that risks to the rights and privacy of

	<p>individuals are minimised while allowing the aims of the project to be met whenever possible.</p> <p>This policy provides a standardised approach towards identifying, assessing and mitigating data protection and privacy risk and assists towards the delivery of compliance with legal statutory requirements.</p>
Information Governance Policy for SystmOne and Summary Care Record	<p>The purpose of this policy and procedure is to ensure that the removal and viewing of information within patients' electronic records on SystmOne, meets the requirements of the Caldicott Principles.</p> <p>It is also to provide guidance for the processing of Tasks received in SystmOne, advising of a clinician overriding the patients' previously agreed consent/dissent to view records.</p>
Subject Access Request Policy	<p>The purpose of this policy and procedure is to ensure that there is a clear approach to the processing of all requests for access to records, throughout the Organisation. To provide confidence to operational staff dealing with subject access request queries.</p>
Freedom of Information Requests Policy	<p>This Policy informs ECCH staff and contractors of the procedure to follow when in receipt of a Freedom of Information request.</p>
Records Management Policy & Procedure	<p>The purpose of this policy is to set out a framework within which employees responsible for managing the Organisation's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and in accordance with legal, operational and information needs. The document also clarifies the actions required of all employees to achieve good quality records management.</p>
Information Security Incident and Incident Investigation Policy	<p>The Purpose of this policy document is to ensure that staff are aware of their individual responsibilities in relation to Security Incidents and the Investigation of the CIC's systems</p>

2. PURPOSE

The purpose of this policy is to provide details of the framework for implementation of the Information Governance (IG) Strategy to enable ECCH to meet its responsibilities for the management of information assets and resources

3. SCOPE

This policy applies to all East Coast Community Healthcare staff members, whether permanent, temporary, or contracted in (either as an individual or through a third party supplier).

This policy covers Information Governance matters in relation to all of the information assets of East Coast Community Healthcare. There are many types of information asset that ECCH is responsible for, including: patient information; databases and data files; contracts and agreements; system documentation; research information; user manuals; training material; operational or support procedures; business continuity plans; fallback arrangements; audit trails; and archived information; specifically:

- software assets: application software, system development tools, and utilities.
- physical assets: computer equipment, communications equipment, removable media, and other equipment.
- services: computing and communications services, general utilities, e.g., heating, lighting, power, and air-conditioning.
- people, and their qualifications, skills, and experience.
- intangibles, such as reputation and image of the organisation.

4. DEFINITIONS

The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Term	Definition
Information Governance (IG)	Information Governance (IG) is about how to manage and share information or data appropriately.
Confidentiality	Confidentiality is a set of rules that limits access or places restrictions on the use of certain types of information.
Information Asset (IA)	An information asset has been defined by the National Archives as “A body of information, defined and managed as a single unit, so that it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.”
Data Protection Act (DPA)	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR).
General Data Protection Regulation (GDPR)	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

UK GDPR	The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018. The key principles, rights and obligations remain the same.
---------	---

5. RESPONSIBILITIES

- ECCH Employees** – Are responsible for ensuring that they are aware of the requirements incumbent upon them, and for ensuring that they comply with these policies on a day-to-day basis. All staff contracts and contracts with third parties contain clauses regarding compliance with Information Governance and Confidentiality guidelines. Staff are also provided with a Staff Handbook at their induction which also gives guidance on compliance with Information Governance and Confidentiality guidelines.
- Chief Executive of ECCH** – Overall responsibility for the enforcement of this policy lies with the Chief Executive of ECCH
- ECCH Line Managers** – Are responsible for ensuring that all policies are adhered to, and, where required, are built into local processes, and for ensuring there is on-going compliance with them. Line Managers are also responsible for ensuring that all IG compliance and training requirements are cascaded to staff members.
- Senior Information Risk Owner (SIRO) – Executive Director of Finance and Resources:** The Senior Information Risk Owner (SIRO) on behalf of the Board. The SIRO owns the information risk and incident management framework, overall information risk approach and risk assessment processes, and is responsible for ensuring they are implemented consistently.
- Caldicott Guardian (CG)** Is the senior person responsible for protecting the confidentiality of personal confidential data (PCD) and information. The Caldicott Guardian plays a key role in ensuring that ECCH and partner organisations abide by the highest level of standards for handling PCD and personal identifiable information (PII).
- Data Protection Officer (DPO) - Risk & Information Governance Team Lead:** Is a legal role required by the GDPR. This person is responsible for overseeing the Information Governance (IG) Policy and Framework and the implementation of data protection and security measures to ensure compliance with the GDPR requirements; these measures should ultimately minimise the risk of breaches and uphold the protection of PII and special categories of data.
- ECCH Information & Caldicott Governance Group** - Is responsible for overseeing day-to-day IG issues, developing and maintaining policies, procedures and guidance documents, co-ordinating and raising awareness of IG within at ECCH, and for monitoring IG incidents and risks. Responsibility for the operation of the IG Group lies with the Risk and Information Governance Team Lead.

6. POLICY STATEMENT

ECCH recognises the need for the right balance between openness and confidentiality in the management and use of information. The Organisation supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

7. PROCEDURE

The key interlinked strands to the IG Policy & Framework are:

- Openness
- Legal Compliance
- Information Security
- Information Quality Assurance
- Training & Support

Openness

- Non-confidential information of ECCH and its services should be made routinely available to the public in accordance with the Freedom of Information Act (2000).
- The East Coast Community Healthcare, as CIC is not a public body and is not, therefore, required to comply with the Freedom of Information Act (FOI), however will review all FOI requests on an individual basis in line with ECCH's FOI policy.
- The Duty of Candour is a legal duty of a hospital, community, and mental health trusts to inform and apologise to patients if there have been mistakes in their care that have led to significant harm. Duty of Candour aims to help patients receive accurate, truthful information from health providers.
- ECCH are therefore duty bound, should anything we do cause a patient significant harm or should we make mistakes in care or care delivery, including information governance, to explain the issue in full to the patient. Where a patient is identified as lacking capacity to fully understand the harm or mistake their family/carers will be advised in their best interest.

Legal Compliance

- ECCH regards all personal data about individuals and commercially sensitive data as confidential. Confidential data must be processed in accordance with the Human Rights Act (1998), Data Protection Act (2018), and the Common Law Duty of Confidentiality.
- ECCH Confidentiality Policy is the record which guides staff members in the legal framework that the organisation must comply with when processing confidential information. This policy also contains East Coast Community Healthcare's policy on Data Protection and the confidentiality component of Information Security.

Responsibility for the implementation of this policy lies with the Risk and Information Governance Team Lead.

Information Security

- Information Security is fundamental to the operation of ECCH due to the confidential data it processes and the reliance on *information* systems to process and transmit data to the organisation's stakeholders. A risk-based approach to information security is adopted by ECCH in line with the requirements laid down by BS ISO/IEC 27001:2005, the British Standard for Information Security Management.
- The East Coast Community Healthcare Information Security Policy is the record which guides staff members in the information security policy framework. Responsibility for the implementation of this policy lies with the Head of Information Security.

Information Quality Assurance

- All staff members are expected to take ownership of, and seek to improve, the quality of information used within their business area.
- Wherever possible, information should be accurate and up-to-date, free from duplication and quality assured at the point of collection.
- ECCH's Records Management Policy is the record, which defines our Records Management (RM) policy and guides staff members in the process of how to manage records during their lifecycle from initial creation, filing, tracking, retention, storage, and disposal of records, in a way that is administratively and legally sound. Responsibility for the implementation of this policy lies with the Risk and Information Governance Team Lead.

Training and Support

- Staff awareness is critical to the success of IG at ECCH.
- IG training must be provided as part of the staff induction process when staff join the organisation. All new starters are to complete the Introduction to Data Security eLearning course accessed via ECCH eLearning system (ESR). This requirement will be expected to be undertaken within one month of their start date of employment at East Coast Community Healthcare. Managers are responsible for managing staff are required to comply with this requirement. If the staff member joining ECCH has an NHS Passport which provides evidence of up-to-date Information Governance Training this will be accepted in place of the Introduction course.
- Data Security training must be part of an annual mandatory training Programme where staff can update their current knowledge. All staff (including clinical and non-clinical) will complete an annual mandatory Data Security Refresher module accessed via ECCH eLearning System (ESR).

- Key staff are given additional training to perform their role. For staff in designated roles (e.g., the SIRO, Caldicott Guardian, DPO etc.) an annual training needs analysis (TNA) will be produced and shared with the relevant staff. Those in specialised roles will undertake relevant training/development in line with the TNA.
- IG training should form part of the annual staff appraisal or performance review of staff.
- Training must be provided whenever there is a change in role or responsibilities.
- Further IG training is identified following the Incident & Risk Management System investigation relating to an information governance incident.
- IG will form part of the Learning and Development, Statutory and Mandatory Framework.
- A blended learning approach is provided to staff members, using the following:
 - Data Security Mandatory Training - ESR
 - ECCH's IG Handbook and Policies -ECCHO
 - IG Awareness Communication Materials

8. MONITORING AND REVIEW

This Policy will be reviewed every 3 years or in case of legislation change at an earlier date.

9. REFERENCES

- <https://www.dsptoolkit.nhs.uk/>
- <https://digital.nhs.uk/>
- <https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr>
- <https://ico.org.uk/>
- <https://www.england.nhs.uk/ig/>

10. ASSOCIATED POLICIES & PROCEDURES *(To include but not limited to)*

- Information Governance (IG) Handbook
- Data Protection & Personal Information Handling Policy
- Confidentiality Policy
- Information Governance Policy for SystmOne and Summary Care Record
- (RA)Registration Authority and NHS CRS Smartcard Policy
- Data Protection & Impact Assessment Policy & Procedure
- Subject Access Request Policy
- Freedom of Information Requests Policy
- IT Security Policy
- Information Security Incident and Incident Investigation Policy
- Mobile Solutions Policy
- Records Management Policy & Procedure
- Record Keeping Policy

- Video Interactive Guidance Policy
- Incident Reporting Policy

11. **AUTHOR**

Data Protection Officer – February 2023

12. **APPENDICES**

1. Appendix – Senior Information Governance Roles and Responsibilities

Role	Designated Officer	E-mail
Risk and Information Governance Team Lead and Data Protection Officer (DPO)	Hannah Lewis	hannah.sewell@ecchcic@nhs.uk
Information Security Lead (Cyber Security)	Martin Green	martin.green@ecchcic.nhs.uk
Caldicott Guardian	Geraldine Rodgers	geraldine.rodgers@ecchcic.nhs.uk
Senior Risk Information Owner (SIRO)	Simon Bragg (Deputy Chief Executive and Executive Director of Finance and Resources)	simon.bragg@ecchcic.nhs.uk

2. Appendix – Equality & Diversity Impact Assessment

In reviewing this policy, the Group considered, as a minimum, the following questions:

- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so is this planned?

Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation.

3. Appendix – Documents Control Sheet

Name of Document:	Information Governance Policy and Framework
Version:	2.6
File Location / Document Name:	ECCHO
Date Of This Version:	February 2025
Produced By (Designation):	Risk and Information Governance Team Lead - DPO
Reviewed By:	Risk and Information Governance Team Lead - DPO
Synopsis And Outcomes of consultation Undertaken:	
Synopsis And Outcomes of Equality and Diversity Impact Assessment:	No impact
Ratified By (Committee):-	Information Governance & Caldicott Group
Date Ratified:	27/02/2025 - Information Governance & Caldicott Group
Distribute To:	ECCHO
Date Due For Review:	February 2028
Enquiries To:	Information Governance Lead DPO
Approved by Appropriate Group/Committee	✓ Date: 27/02/2025 - Information Governance & Caldicott Group

4. Appendix – Version Control

Version Date	Version No.	Author/ Reviewer	Comments
1	25/05/2012	IG Admin	Draft for Approval
1.1	25/01/2014	IG Admin	Approved by Board
2	10/2016	BI Team	Updated for 2016
2	March 2018	Andy Thornton	Periodic Review
2.1	February 2020	R & IG Team Lead, Data Protection Officer	Periodic Review – amended job titles & roles & responsibilities
2.2	March 2021	R & IG Team Lead, Data Protection Officer	Amended year Typo DPA 1998 changed to 2018
2.3	February 2022	R & IG Team Lead, Data Protection Officer	Full Review & New Template *Updated Responsibilities – Added SIRO, DPO, CG *Added References * Updated training section to include annual TNA *Added definitions * Added to introduction policies which sit under the IG umbrella to explain them *Added purpose
2.4	July 2022	Head of Corporate Governance & Risk Management – DPO	References to Datix amended to ECCH's Incident & Risk Management System
2.5	February 2023	Head of Corporate Governance and Risk Management / <u>Data Protection Officer</u>	Name change to Caldicott Guardian and Information Security Lead. Added additional line into handbook about not using personal devices for work purposes.
	Nov 2024	Head of Corporate Governance and Risk Management / Data Protection Officer	Name change to Caldicott Guardian
2.6	Feb 2025	Head of Corporate Governance and Risk Management / Data Protection Officer	Reviewed and updated policy. Changed references to Access to Health Records Policy to Subject Access Request Policy. Handbook updated examples of incidents added – 'Looking at a record without a valid reason.' DPIA guidance updated to include form now on QUEST.

5. Appendix – IG Handbook





This Handbook is a reference and guide to signpost you to the ECCH's Information Governance Policies & Procedures which can be accessed via ECCHO.

ECCH is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment. This document can only be considered valid when viewed via ECCHO. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.



Contents

(For quick access to a specific heading - press CTRL and click your mouse to follow the link for the below options)

Introduction	18
What YOU need to know about Information Governance	18
Information Security	19
Keeping Information Safe	20
Incident Reporting Procedure	21
Information Governance requirements for New Processes, Services and Systems	22
NHS Care Records Smartcard	22
Confidentiality	9
Information Leaks Loss	10
Guide to Confidentiality in Health and Social Care	11
Revised Caldicott Principles	11
Information Sharing	12
Secure Transfer of Information Guidance	13
Records Management	13
Data Quality	14
Data Protection	14
Freedom of Information	16
Information Commisioners Office	19
Where to get training	19
Definitions & Abbreviations	20
Key Information Governance Contacts	22
Associated Policies & Procedures	23
Your Information Governance Declaration	24
Document Approval & Version Control	25

Introduction

Information is the lifeblood of an organisation and one of its most valuable assets.

Information Governance provides a framework for the handling of that information, in particular, the handling of person-identifiable and confidential information in a secure and confidential manner.



What YOU need to know about Information Governance

The Information Governance framework determines how we collect and store data and specifies how the data is used and when it can be stored.

Everyone who works for or on behalf of ECCH (*including temporary, contract, remote, mobile, remote workers and volunteers*) must be aware of:

- The importance of the information we hold which may be confidential or sensitive and relate to patients, staff, ECCH or its partners (Business Sensitive).
- The legislation, guidance and best practice for looking after such important information.
- Why YOU must take responsibility for how you obtain, record, use, keep and share information.
- The impact Information Governance has on our Business Continuity Management and our ability to continue to serve patients.

All staff, whether permanent, temporary or contracted, are responsible for making themselves aware of ECCH's Information Governance duties and obligations, and for complying with these on a day to day basis. Please familiarise yourself with ECCH's Information Governance policies and associated guidance, available on ECCHO. (*A full list is available at the end of this Handbook*)

Information Governance is
EVERYONE's
responsibility



Information Security

All staff are accountable for information security and must understand and comply with ECCH's **IT Security Policy** and associated guidance.



The aim of ECCH's IT Security Policy is to preserve:

Confidentiality	Access to Data shall be confined to those with appropriate authority.
Integrity	Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
Availability	Information shall be available and delivered to the right person, at the time when it is needed.

The **Senior Information Risk Owner (SIRO)** is responsible for information risk within ECCH and advises the Board on the effectiveness of information risk management across the organisation.

DOs

- ✓ **Do** understand what information you are using, how it should be protectively handled, stored and transferred
- ✓ **Do** understand the procedures, standards, and protocols for the sharing of information with others
- ✓ **Do** know how to report a suspected breach of information security within the ECCH
- ✓ **Do** be aware of your responsibility for raising any information security concerns with the IG team in the first instance.
- ✓ **Do** ensure that all ECCH mobile devices (e.g. laptop, mobile phones) are stored securely at all times and locked away when not in use.
- ✓ **Do** know how to report a loss or theft of ICT equipment

DON'Ts

- ✗ **Don't** share account and/or system password details
- ✗ **Don't** use devices (e.g. laptops) or removable media (e.g. USB sticks) to access ECCH information or systems unless the device is encrypted
- ✗ **Don't** install software on ECCH systems without the prior permission of the IT Department
- ✗ **Don't** allow external contractors (or third parties) to gain access to ECCH information systems without a contract in place ensuring compliance with appropriate ECCH security policies
- ✗ **Don't** interfere with antivirus software installed on ECCH systems or purposefully upload or transmit a known computer virus or item of malicious software to others
- ✗ **Don't** use personal devices for any ECCH work e.g., calls, photos, emails.

Keeping Information Safe

ECCH holds information relating to individuals which must be protected and maintained. All staff need to be aware of their responsibilities in preserving information security and safeguarding confidentiality.

DOs

- ✓ **Do** be aware that email and internet access is provided to support the business, however, occasional and reasonable personal use is permitted, provided that it does not interfere with the performance of duties and does not conflict with ECCH policies
- ✓ **Do** be aware that ECCH has the right to monitor system activity where it suspects that there has been a breach of policy
- ✓ **Do** select a quality password in accordance with password guidance and ensure your password remains confidential
- ✓ **Do** familiarise yourself with how the email guidance
- ✓ **Do** be aware that personal use of corporate mobile devices is not generally permitted, except in exceptional circumstances. Personal use may be logged and excessive use investigated



DON'Ts

- ✗ **Don't** share your user ID or system password with others (e.g. to new or temporary staff)
- ✗ **Don't** send person-identifiable, confidential or sensitive information via e-mail unless it is encrypted. To assist you, your work email is automatically encrypted in transit.
- ✗ **Don't** use ECCH network drive or systems for the installation of games or to store personal music or photographs. ECCH monitors its network drives and systems
- ✗ **Don't** illegally duplicate copyrighted content onto ECCH equipment
- ✗ **Don't** attempt to access/forward material that is defamatory, pornographic, sexist, racist, offensive or on-line gambling

Incident Reporting Procedure

You have a responsibility to identify and report any information governance incidents and information security risks in order for ECCH to investigate, learn from them and implement new systems or processes to mitigate the risk of further incidents occurring.



All Information Governance (IG) Incidents must be reported immediately to

- ✓ Your Line Manager
- ✓ On Incident & Risk Management System incident reporting system QUEST

Information Governance Incidents can apply to the loss of both electronic media and paper records.

Examples of IG Incidents Include but are not limited to the below list:

- ✓ *Lost or stolen mobile working device e.g. laptop/mobile*
- ✓ *Letter is found left lying around or on the printer*
- ✓ *Email sent to the wrong person/organisation*
- ✓ *Information entered into the wrong patient record*
- ✓ *Letter/Information sent to the wrong patient*
- ✓ *A staff record is sent to the wrong recipient*
- ✓ *Looking at a record without a valid reason*

An Information Governance Serious Incident Requiring Investigation (SIRI) is any incident involving the actual or potential loss, theft or unauthorised disclosure of person-identifiable information which could lead to identity fraud or have other significant impact on individuals.

Please note that if ECCH has to report any serious incident to the Information Commissioners Office (ICO) we only have 72 hours to do so, therefore prompt reporting is imperative.

Your **Data Protection Officer (DPO)** or **Senior Information Risk Owner (SIRO)** or **Caldicott Guardian** must be informed of such incidents, as appropriate, to enable an investigation to be carried out. There may be extra reporting mechanisms that the ECCH must comply with as a result of an incident.

Please note any incidents regarding stolen equipment e.g. stolen laptop, should be reported to the **IT Service Desk**. On Incident & Risk Management System and to your Line Manager to ensure that all relevant people within ECCH have been informed of the incident.

All IG incidents reported on to Incident & Risk Management System are reviewed by the Data Protection Officer (DPO) and reported on weekly at the incident review group and BI monthly and the Information Governance and Caldicott Group. The DPO will liaise with the Incident & Risk Management System incident handler to ensure all appropriate action is taken to resolve the incident and mitigate the risk of reoccurrence.

Information Governance requirements for New Processes, Services and Systems

ECCH needs to ensure that when new processes, services, systems and other information assets are introduced, the implementation does not result in an adverse impact on privacy, information quality or a breach of information security, confidentiality or data protection requirements.

For best effect, requirements to ensure information security, confidentiality and data protection and information quality should be identified and agreed prior to the design, development and/or implementation of a new process or system. All staff members who may be responsible for introducing changes to services, processes or information assets must be aware of the requirement to consider information governance requirements.

All new projects likely to involve a new use or significantly change the way personal information is handled must have a Data Protection Impact Assessment (DPIA) undertaken. This will ensure all IG requirements are considered and any risks mitigated.

For further information on ECCH's [Data Impact Assessment \(DPIA\) Policy & Procedure](#) go to ECCHO – Policies and Procedures. A DPIA form is available on QUEST, please contact the DPO for any guidance. Useful guidance can also be found on the ICO's website.



NHS Care Records Smartcard

It is important that all Smartcards users follow the conditions of the Smartcard in the [Smartcard & Registration Authority Policy](#) which can be found on ECCHO under Policies and Procedures.

DOs

- ✓ **Do** remember that any work done under your Smartcard log-in will be attributed to you



DON'Ts

- ✗ Don't log onto the S1 Care Record System and leave your Smartcard unattended — always remove your Smartcard when leaving your workstation
- ✗ Don't share your smartcard/passcode

Mobile Working

When working away from the office environment, the potential risks in relation to loss, damage, theft or unauthorised disclosure of information are increased.



DOs

- ✓ **Do** ensure any equipment supplied by ECCH is used only by you for ECCH business/work
- ✓ Passwords should comply with the latest IT Security Policy found on ECCHO
- ✓ **Do** ensure you back-up and save work undertaken to ECCH systems as soon as you return to the office (is this correct?)
- ✓ **Do** take care when leaving public places/transport/taxis and ensure that you take all equipment and information with you
- ✓ **Do** know how to report a loss or theft of ICT equipment

DON'Ts

- ✗ **Don't** leave ECCH equipment or portable devices on display in your car, ensure they are locked away in your boot
- ✗ **Don't** process person-identifiable or confidential information on your personal computer when working from home
- ✗ **Don't** take person-identifiable or confidential information away from the office environment unless it is an absolute necessity — a risk assessment must be undertaken, and it must be adequately secure
- ✗ **Don't** use a mobile device to work on personal/confidential information in a public place (e.g. on a train), where there is a risk it may be viewed by others
- ✗ **Don't** discuss personal/confidential information in a public place, you may be overheard this includes in the vicinity of smart devices e.g. Alexa

All NHS employees are bound by a legal duty of confidence to protect the personal information they may come into contact with during the course of their work.



DOs

- ✓ **Do** be aware that as an ECCH employee you have signed a contract of employment which contains a confidentiality agreement
- ✓ **Do** safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working for or on behalf of the NHS
- ✓ **Do** be aware of clearing desks of records containing personal confidential data. Storing in appropriate storage places
- ✓ **Do** switch off computers or put them into a password protected mode, if you leave your desk for any length of time
- ✓ **Do** ensure that you cannot be overheard when discussing confidential matters
- ✓ **Do** be vigilant if you are undertaking work away from the ECCH office environment. Ensure you apply suitable transportation methods so that information cannot be over looked by or is in view of others
- ✓ **Do** be aware that the NHSmail address book contains many similar staff names and you must therefore ensure that information is sent to the intended recipient
- ✓ **Do** challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential business information and ensure they have a need to know
- ✓ **Do** use only the minimum information necessary
- ✓ **Do** seek advice if you need to share patient/person-identifiable Information without consent of the patient/person to which the information relates, and record the decision and any action taken
- ✓ **Do** report any actual or suspected breaches of confidentiality
- ✓ **Do** use the confidential waste bins to dispose of any document containing person identifiable or confidential information, whether or not you consider it to be confidential

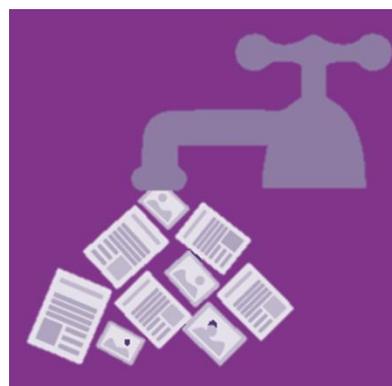
DON'Ts

- ✗ **Don't** share passwords or leave them lying around for others to see
- ✗ **Don't** share information without the consent of the person to which the information relates, unless there are statutory grounds to do so
- ✗ **Don't** use person-identifiable information unless absolutely necessary. Anonymise the information where possible
- ✗ **Don't** collect, hold or process more information than you need and do not keep it for longer than necessary
- ✗ **Don't** transfer person-identifiable or confidential business information unless absolutely necessary. If it is necessary transfer the information by secure means i.e. use an your work email e account

Information Leaks/Loss

As well as person-identifiable information ECCH also holds confidential corporate/business information and it is vital that this is not disclosed without authority to do so.

It is your responsibility to ensure the highest level of care when handling confidential information to prevent leaks.



Guide to Confidentiality in Health and Social Care

Staff must also adhere to the rules laid out in the '**A Guide to Confidentiality in Health and Social Care**' – available via the NHS Digital website - <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care>

Rule 1 – Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2 – Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3 – Information that is shared for the benefit of the community should be anonymised

Rule 4 – An individual's right to object to the sharing of confidential information about them should be respected

Rule 5 – Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

Revised Caldicott Principles

The Caldicott Review was about striking the right balance between sharing people's health and care information to improve services and develop new treatments while respecting the privacy and wishes of the patient. Many of the recommendations in the review echo the commitments made in the NHS Constitution. The revised Caldicott principles offer a new opportunity to promote information governance throughout the health and social care system and challenge a culture that undermines the quality of patient care by failing to share information effectively.

The revised **8 Caldicott Principles** to ensure people's information is kept confidential and used appropriately are listed below:



Principle 1: *Justify the purpose(s) for using confidential information*



Principle 2: *Use confidential information only when it is necessary*



Principle 3: *Use the minimum necessary confidential information*



Principle 4: *Access to confidential information should be on a strict need-to-know basis*



Principle 5: *Everyone with access to confidential information should be aware of their responsibilities*



Principle 6: *Comply with the law*



Principle 7: *The duty to share information for individual care is as important as the duty to protect patient confidentiality*



Principle 8: *Inform patients and service users about how their confidential information is used*

Information Sharing

Person-identifiable information sometimes needs to be shared with other organisations and/or third parties. Information that is shared for the direct care of an individual is generally shared with the informed consent of the data subject. However, there are circumstances where it is both legal and appropriate to share information without consent or where consent may be over-riden.

For example:

- In the vital (life or death) interest of the data subject or another person and consent cannot be obtained
- Safeguarding of children or vulnerable adults
- By order of the Secretary of State
- In connection with a serious crime
- Where the public interest outweighs the duty of confidentiality



It is good practice to have data sharing agreements in place particularly where information is to be shared on a large scale or on a regular basis. For further information contact the DPO.

Where possible personal data should be anonymised for sharing e.g. for research or other data analysis purposes. For further details see: **ICO Anonymisation Code of Practice**
For further good practice recommendations on data sharing see the ICO Data Sharing Code of Practice

Remember the 7 golden rules for Information Sharing:

1. Remember that the data protection act is not a barrier to information sharing
2. Be open and honest
3. Seek advice
4. Share with consent where appropriate
5. Consider safety and well-being
6. Necessary, relevant, proportionate, accurate, timely and secure
7. Keep a record

Secure Transfer of Information Guidance

ECCH have Secure Transfer of Information Guidance for flows of confidential information which must follow the Caldicott Principles. ECCH has a corporate responsibility to ensure that Safe Haven administrative arrangements are in place to safeguard confidential person- identifiable information so that it can be handled and communicated safely and securely.

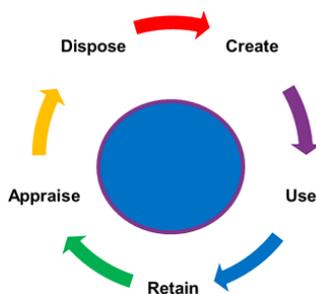
All routine transfers/flows of person-identifiable, confidential and sensitive information should be subject to a risk assessment and procedures should be in place to ensure receipt at a secure and protected point.

Safe Haven Procedures act as a safeguard for confidential information which enters or leaves the organisation, whether this is by e-mail, post or other means.

Any members of staff handling confidential information, whether paper based or electronic must adhere to the IT Security Policy.

Records Management

Records Management covers the full lifecycle of a record from creation through to disposal and is the term used to cover ECCH processes in order to meet its legal and regulatory requirements



Records management is crucial to ECCH; unless records are managed efficiently, it is not possible to conduct business, to account for what has happened in the past or to make decisions about the future. Records come in many formats including emails, paper, digital documents, digital images, social media, CD's and blogs and, are a vital, corporate asset which are required to:

- provide evidence of actions and decisions
- support accountability and transparency
- comply with legal and regulatory obligations, including employment, contract and financial law, as well as the Data Protection Act and Freedom of Information Act
- support decision making
- protect the interests of staff, patients and other stakeholders

Records must be retained for set periods of time and destroyed under appropriate confidential conditions, in accordance with **ECCHs Records Management Policy & Procedure** which can be found on ECCHO.

Data Quality

Data quality is essential for the availability of complete, accurate and timely data. It is required in supporting patient care, clinical governance and service level agreements.

All staff who record information, whether by paper or by electronic means, have a responsibility to take care to ensure that the data is accurate, legible and as complete as possible. The data needs to be present at the time that processes require it, for both service delivery and reporting purposes.

Staff are responsible for the data they enter onto any ECCH system. We have to keep personal and public information accurate and up to date to comply with the Data Protection Act 2018

Data Protection

ECCH needs to process personal data about people in order to operate. These include current, past and prospective patients, staff, suppliers and business contacts.

There are legal safeguards to ensure the personal data is handled appropriately. Under the Data Protection Act (DPA) 2018 anyone has the right to see and have a copy of information about them which is held by ECCH, this is known as a Subject Access Request (SAR). All requests must go through the Quality Team and should never be sent out from an individual service.

ECCH fully complies with the eight **Data Protection Principles** which specify that personal data must:

- 📁 be processed fairly and lawfully
- 📁 be obtained only for one or more specified and lawful purposes
- 📁 be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed
- 📁 be accurate and, where necessary, kept up to date
- 📁 not be kept for longer than is necessary
- 📁 be processed in accordance with the rights of data subjects
- 📁 have appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- 📁 not be transferred outside the European Economic Area (EEA) without adequate protection

DOs

- ✓ **Do** understand and comply with the eight DPA principles
- ✓ **Do** observe all ECCH guidance, codes of practice and procedures concerning the collection and use of person-identifiable information
- ✓ **Do** think about person-identifiable Information held as though it were held about you – respect confidentiality and the rights of the data subject
- ✓ **Do** ensure you have a contract in place when sharing person- identifiable information

DON'Ts

- ✗ **Don't** leave person-identifiable information insecure, whether paper files or electronic Information
- ✗ **Don't** erase or alter person- identifiable information which is the focus of a Subject Access Request
- ✗ **Don't** change the purpose without permission from the data subject
- ✗ **Don't** store outside EEA

Freedom of Information

The Freedom of Information Act 2000 (FOI) gives members of the public the right to access information held by a public authority.

The general principle is that all information held by ECCH may be disclosed, except for a small number of tightly defined exempt items. For further information please see **ECCH's Freedom of Information Policy** available via ECCHO – Policies & Procedures.

The Act is applicant and motive blind. This means that it does not matter who the requester is or why they want the information - the applicant does not need to give a reason.

A request can be made to anybody in ECCH so it's everyone's responsibility to know how to handle requests. We also have to respond to requests about the environment (e.g. air, water, soil, land, emissions, etc.) under the Environmental Information Regulations 2004 (EIR) in the same way that we deal with FOI requests.

**All requests should be directed without delay to:
ECCH's Data Protection Officer & Communications Team**

DOs

- ✓ **Do** be mindful of the information you hold and where it is kept
- ✓ **Do** refer to the FOI policy
- ✓ **Do** remember that **all** information held is subject to the FOI Act, including draft documents and is subject to disclosure. As such, any content should be written in a professional manner
- ✓ **Do** act promptly when asked to provide information in response to a request
- ✓ **Do** advise the DPO and Communications Team if you consider that some or all of information requested may be subject to an FOI exemption (e.g. if the information is personal data or commercially sensitive)

DON'Ts

- ✗ **Don't** delete any information subject to a Freedom of Information request – it is a criminal offence to knowingly amend or destroy information subject to an FOI request
- ✗ **Don't** withhold information subject to an FOI request. It is important that you provide the FOI Team with all information requested. The information you provide may not be required to be disclosed, however, withholding information may affect the response

Information Commissioner's Office

The Information Commissioner's Office (ICO) is the independent authority set up to uphold information rights in the public interest, promoting openness by public authorities and data privacy for individuals.

The ICO can prosecute an organisation for serious breaches of the Data Protection Act or Privacy and Electronic Communications Regulations and has the power to fine a data controller (such as NHS England) up to £500,000. Recent fines and undertakings by the ICO include:

NHS Surrey - fined £200,000 over the loss of sensitive information about more than 3,000 patients.

Brighton and Sussex University Hospitals NHS Foundation Trust fined £325,000 after "highly sensitive personal data" was stolen from a hospital under its control and sold on eBay.

St. George's Healthcare NHS Trust, London fined £60,000 after an individual's medical information was sent to the wrong address.

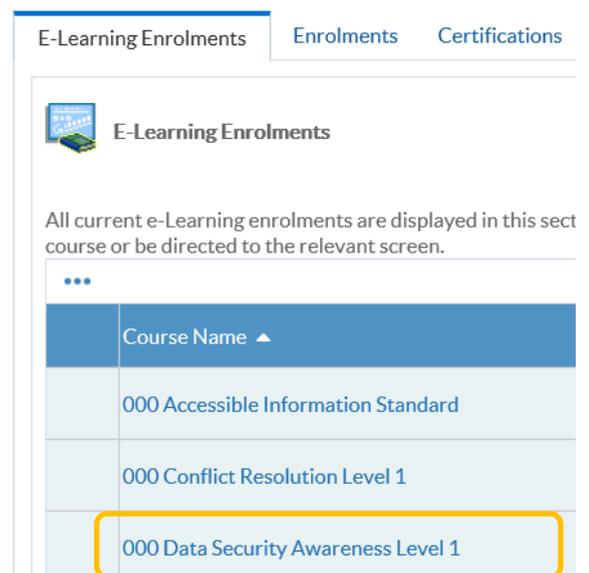
More information about Freedom of Information and Data Protection can be found at www.ico.org

Where to get training

Data Security & Awareness is an E-Learning training module and forms part of your Mandatory Training. This course should be completed as soon as you start ECCH and then annually thereafter.

Staff are accountable for ensuring they complete their training via the ESR portal, guidance on accessing this can be found: ECCHO-OD & Training – **E-Learning – 'ESR E-Learning Self-Help Guide'**.

If you are a Manager you will receive a mandatory training compliance report monthly and should also monitor your staff's compliance.



The screenshot shows a web interface for 'E-Learning Enrolments'. At the top, there are three tabs: 'E-Learning Enrolments', 'Enrolments', and 'Certifications'. Below the tabs, there is a header 'E-Learning Enrolments' with a small icon. A message states: 'All current e-Learning enrolments are displayed in this section or be directed to the relevant screen.' Below this is a table with a blue header row 'Course Name ▲'. The table contains three rows of course names: '000 Accessible Information Standard', '000 Conflict Resolution Level 1', and '000 Data Security Awareness Level 1'. The last row is highlighted with a yellow border.

Course Name ▲
000 Accessible Information Standard
000 Conflict Resolution Level 1
000 Data Security Awareness Level 1

Definitions & Abbreviation List

Full Term	Abbreviation	Definition
Data Protection Act	DPA	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General
General Data Protection Regulation	GDPR	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area
European Economic Area	EEA	The European Economic Area, abbreviated as EEA, consists of the Member States of the European Union (EU) and three countries of the European Free Trade Association
Freedom of Information	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities.
Information Asset Owner	IAO	The owner is responsible for establishing the controls that provide the security and authorizing access to the information resource.
Information Commissioner's Office	ICO	The Role of the Information Commissioner's Office (ICO) in Relation to the GDPR. The Information Commissioner's Office (ICO) is the independent regulatory office in charge of upholding information rights in the interest of the public.
Information Governance	IG	Information governance is a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset.
Personal Confidential Data	PCD	Name, surname, phone number, address, social security number, religious or sexual orientation – all are sensitive personal data.
Data Protection Impact Assessment	DPIA	A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. You must do a DPIA for processing that is likely to result in a high risk to individuals
Subject Access Request	SAR	A subject access request (SAR) is a written request made by or on behalf of an individual for the information which they are entitled to ask for.
Data Protection Officer	DPO	The Data Protection Officer is a legal role required by the GDPR. This person is responsible for overseeing the Information Governance (IG) Policy and Framework and the implementation of data protection and security measures to ensure compliance with the GDPR requirements; these measures should ultimately minimise the risk of breaches and uphold the protection of PII and special categories of data.

Senior Information Risk Owner	SIRO	The Senior Information Risk Owner (SIRO) on behalf of the Board. The SIRO owns the information risk and incident management framework, overall information risk approach and risk assessment processes, and is responsible for ensuring they are implemented consistently.
Caldicott Guardian		The Caldicott Guardian is senior person responsible for protecting the confidentiality of personal confidential data and information. The Caldicott Guardian plays a key role in ensuring that ECCH and partner organisations abide by the highest level of standards for handling personal information and personal identifiable information
Business Sensitive Information		Business information: Sensitive business information includes anything that poses a risk to the company in question if discovered by a competitor or the general public. Such information includes trade secrets, acquisition plans, financial data and supplier and customer information, among other possibilities.
Personal Data		Means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Encrypted		Encryption is the method by which information is converted into secret code that hides the information's true meaning.
Anonymised		Anonymised data means that all identifiers have been irreversibly removed and data subjects are no longer identifiable in any way.
Third Party		Any person other than; Data Protection & Personal Information Handling Policy Version 8 Issued: October 2016 Amended April 2021 Review Date: May 2023 Page 9 of 21 (a) the data subject, (b) the data controller or (a) any data processor or other person authorised to process data for the data controller or processor

Key Information Governance Contacts

Information Governance Lead & Data Protection Officer (DPO)	Hannah Sewell	hannah.sewell@ecchcic.nhs.uk
Senior Information Risk Owner (SIRO)	Simon Bragg	simon.bragg@ecchcic.nhs.uk
Caldicott Guardian	Geraldine Rodgers	geraldine.rodgers@ecchcic.nhs.uk
ECCH's IT Helpdesk	IT Helpdesk	ict@ecchcic.nhs.uk
Quality Team Subject Access Requests	SARS	subjectaccessrequest@ecchcic.nhs.uk

Associated Policies & Procedures

The Information Governance Do's and Don'ts throughout this Handbook provide you with a brief introduction to Information Governance in a handy reference tool to support you in your work, signposting you to ECCH Information Governance policies, procedures, guidance, e-learning and useful contacts. All the documents can be found on the ECCHs internal intranet, ECCHO: <http://eccho/Home.aspx>

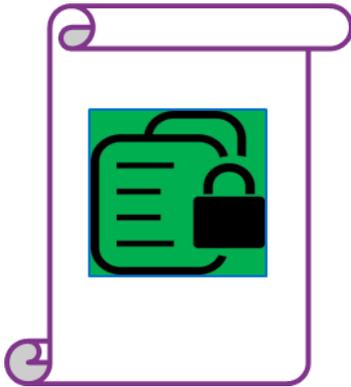
(Relevant Tabs include: 'Policies / Procedures', 'Information Governance, OD & Training')



The below is a comprehensive list of all associated policies available on ECCHO under 'Policies / Procedures'

Policies	
1.	Information Governance Policy & Framework
2.	Data Protection & Personal Information Handling Policy
3.	Confidentiality Policy
4.	Information Governance Policy for SystmOne and Summary Care Record
5.	(RA)Registration Authority and NHS CRS Smartcard Policy
6.	Data Protection & Impact Assessment Policy & Procedure
7.	Subject Access Request Policy
8.	Freedom of Information Requests Policy
9.	IT Security Policy
10.	Information Security Incident and Incident Investigation Policy
11.	Mobile Solutions Policy
12.	Records Management Policy & Procedure
13.	Record Keeping Policy
14.	Reporting Safety Events Policy
15.	PSIRF Plan

Your Information Governance Declaration



All ECCH staff are required to read, understand and agree to the **Information Governance Handbook**. It is your responsibility to learn about Information Governance, to help ensure you follow best practice guidelines to ensure the necessary safeguards for, and appropriate use of person-identifiable and confidential information.

If you require any advice or further information, contact your Data Protection Officer (DPO) - we are here to help you.

This Information Governance Handbook has been developed to ensure that ECCH staff and third parties handling person-identifiable and confidential information are compliant with, but not limited to, the following legislation and regulation standards:

- Data Protection Act (2018)
- Freedom of Information Act (2000)
- Environmental Information Regulations (2004)
- Access to Health Records Act (1990)
- NHS Confidentiality Code of Practice (2003)
- Caldicott Principles (1997)
- Care Records Guarantee – NHS Digital
- Human Rights Act (1998)
- Information Security Standard ISO27001
- Computer Misuse Act (1990)

Please remember that your computer and any ECCH System login has been assigned to you only. As such, you are accountable for your computer and/or ECCH System login and for ensuring that all activity is auditable. It is your responsibility to ensure that password access is known only to yourself and that if you leave your PC/laptop logged on and unattended you must activate a password protected screensaver (press **Ctrl+Alt+Del** on the keyboard lock your workstation) to maintain security and prevent unauthorised use of your PC/laptop.

You should be aware that inappropriate use, including any violation of ECCH Information Governance policies referenced in this handbook, may result in the withdrawal of the facility, prosecution and/or disciplinary action, including dismissal, in accordance with the ECCH disciplinary procedures.