East Coast Community Healthcare (ECCH) (IG) Information Governance Hand book

This handbook as a reference to signpost you to the
ECCH's Information Governance policies, procedures & guidance.

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.

Approving Committee	**Policy Group**
Date Approved	**20/09/2019**
First Review Date	**Aug 2019**
Next Review Date	**Aug 2021**
Policy Author	**Clinical Quality Manager**
Version Number	**V1.1**

Version Control Sheet

Version	**Date**	**Reviewed By**	**Comment**
V1.1	14/05/2020	Hannah Lewis IG Lead	Amended IG Lead and Caldicott Guardian Details
V1.2	16/03/2021	Hannah Lewis IG Lead	Added 8th Caldicott Principle

Analysis of Effect completed:	By:	Date:

Information Governance Handbook Contents

This handbook highlights important Information about Information Governance that you need to familiarise yourself with.

Contents

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

This 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 and remote workers***) 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.
- 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

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 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

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, nhs.net email is automatically encrypted in transit, therefore, any e-mail sent from one NHSmail account to another NHSmail account is secure
- ✗ **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 and learn from them.

All Information Governance **Incidents** must be reported immediately to your line manager and on the Datix reporting system. If ECCH has to report these to the Information Commissioners Office (ICO) we only have 72 hours to do so.

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

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 (e.g. you find a confidential letter on a photocopier, or a lost or stolen NHS laptop).

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 Datix and to your Line Manager to ensure that all relevant people within ECCH have been informed of the incident.

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) undertake. This will ensure all IG requirements are considered and any issues resolved.

NHS Care Records Smartcard

It is important that all Smartcards users follow the conditions of the Smartcard in the Smartcard & Registration Authority Policy RA01 Form

DO

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

DON'T

- ✗ **Don't** log onto the 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
- ✓ 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 d**iscuss personal/confidential information in a public place, you may be overheard this includes in the vicinity of smart devices e.g. Alexa

Confidentiality

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

Confidentiality 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 nhs.net e-mail account or a secure government domain e.g. gsi.gov.uk

Information Leaks/Loss

As well as person-identifiable information ECCH also holds confidential corporate 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 Socialcare

Staff must also adhere to the rules laid out in the ‘A Guide to Confidentiality in Health and Social Care’ – NHS Digital

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 Principles are set out below.

Principle 1 Justify the purpose(s) for using personal confidential data

Principle 2 Don’t use personal confidential data unless it is absolutely necessary

Principle 3 Use the minimum necessary personal confidential data

Principle 4 Access to personal confidential data should be on a strict need-to-know basis

Principle 5 Everyone with access to personal confidential data should be aware of their responsibilities

Principle 6 Comply with the law

Principle 7 The duty to share information can be 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-ridden.

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

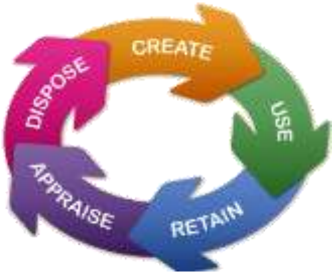
ECCH have Secure Transfer of Information Guidance for flows of confidential information which must follow the Caldicott Principles. ECCH has a corporate responsibility to ensure that Safe Haven administrative arrangements are in place to safeguard confidential person- identifiable information so that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

See the ECCH Records Management Policy for further guidance.

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 1998.

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 without informing the IG team

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.

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 to:
Internal Comms Team
Hamilton House
Battery Green Road
Lowestoft
NR32 1DE
Ecch.comms@nhs.net

DOs

✓ **Do** be mindful of the information you hold and where it is kept

✓ **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 Internal Communication 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.

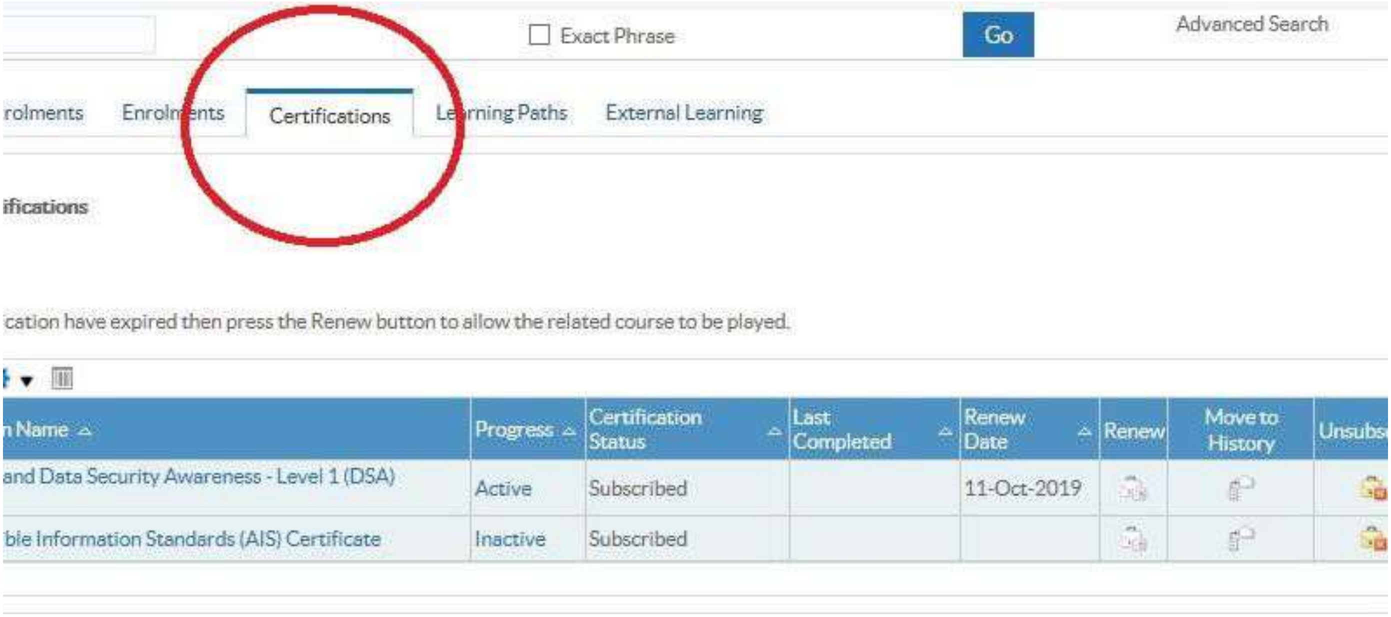
Brighton and Sussex University Hospitals NHS Foundation Trust fined £325,000 after "highly sensitive personal data" was stolen from a hospital under its control and sold on eBay.

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 help and training

If you are new to ECCH please make sure that, as an absolute priority, you complete the e-learning Introduction to Information Governance Mandatory Training Module :



cation have expired then press the Renew button to allow the related course to be played.

n Name	Progress	Certification Status	Last Completed	Renew Date	Renew	Move to History	Unsubs
and Data Security Awareness - Level 1 (DSA)	Active	Subscribed		11-Oct-2019			
ble Information Standards (AIS) Certificate	Inactive	Subscribed					

It is important that you keep up to date with best practice and changes in the legislation.

Abbreviation List

Term/Abbreviation	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing.
DPA	Data Protection Act
EEA	European Economic Area
EIR	Environmental Information Regulations
FOI	Freedom of Information
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
PCD	Personal Confidential Data
DPIA	Data Protection Impact Assessment
SAR	Subject Access Request
SIRO	Senior Information Risk Owner

IG Contact List

IG Team		
Information Governance Lead & Data Protection Officer (DPO)	Hannah Lewis	hannah.lewis15@nhs.net
Senior Information Risk Owner (SIRO)	Simon Bragg	simonbragg@nhs.net
Caldicott Guardian	Paul Benton	paul.benton@nhs.net

Associated Procedures and Guidance

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 website, ECCHO.

Policy/Procedure Name
Information Governance Policy
Data Protection and Personal Information Handling Policy
Confidentiality and Data Protection Policy
Acceptable Use Policy (IT, Email & Internet)
Records Management Policy
Video Interactive Guidance Policy
Confidentiality Policy
Information Governance in SystmOne and SCR
Incident Reporting Procedure and Policy
IT Security Policy
Information Security Incident Policy
Subject Access – Standard Operating Procedure
Freedom of Information Requests

INTEGRITY
AVAILABILITY
SECURITY
CONFIDENTIALITY

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 (i.e.**Ctrl+Alt+Del** 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.