NHS
Bury
Clinical Commissioning Group

Information Governance User Handbook

Version:	3.0
Ratified by:	NHS Bury CCG Information Governance Steering Group
Date ratified:	July 2021
Name of originator /author (s):	NHS England (adapted for NHS Bury CCG); NHS Bury CCG Information Governance Team
Responsible Committee / individual:	NHS Bury CCG Information Governance Steering Group
Date issued:	October 2021
Review date:	July 2022
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Equality Analysis Assessed:	Yes

Further information regarding this document

Document name	Information Governance User Handbook CCG.GOV.029.3.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	NHS England (adapted for NHS Bury CCG); NHS Bury CCG Information Governance Team
This document should be read in conjunction with	All information governance related policies and procedures
This document has been developed in consultation with	NHS Bury Clinical Commissioning Steering Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley St Bury, BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	The corporate PA office CCG Website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
1.0 = Policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	24th September 2015
2.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	15th December 2016
2.3 = review	NHS Bury CCG Information Governance Team	October 2021
3.0 = policy once ratified	NHS Bury CCG Information Governance Steering Group	July 2021

Information Governance User Handbook

Use this handbook as a reference tool to signpost you to the CCG's Information Governance policies, procedures and guidance

Information Governance Handbook Contents

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

Contents

Introduction 4
What YOU need to know about Information Governance 4
Information Security 5
Keeping Information Safe 6
Incident Reporting Procedure 6
Information Governance requirements for New Processes, Services and Systems 7
NHS Care Records Smartcard 8
Mobile Working 8
Confidentiality 10
Information Leaks 11
Guide to Confidentiality in Health and Social care 12
Revised Caldicott Principles 12
Information Sharing 13
Secure Transfer of Information Guidance 13
Audit 14
Records Management 14
Data Quality 15
Data Protection 15
Freedom of Information 17
Information Commissioner's Office 18
Where to get help and training 18
Abbreviation List 19
IG Contact List .....
Information Governance Policies and Associated Procedures and Guidance .....
Your Information Governance Declaration .....

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 the CCG (***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, the CCG 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 the CCG's Information Governance duties and obligations, and for complying with these on a day to day basis. Please familiarise yourself with the CCG's Information Governance policies and associated guidance, available on the internet and listed at the back of this handbook.

Information Governance is EVERYONE's responsibility

Information Security

All staff are accountable for information security and must understand and comply with CCG's Information Security Policy and associated guidance.

The aim of the CCG's Information 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 the CCG and advises the Board on the effectiveness of information risk management across the organisation.

Information Asset Owners (IAOs) are assigned to all the CCG's information assets and are responsible for ensuring that information risk assessments are performed at least annually, or quarterly for key assets.

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 CCG
- ✓ **Do** be aware of your responsibility for raising any information security concerns with the IT Helpdesk
- ✓ **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 CCG information or systems unless the device is encrypted
- × **Don't** install software on CCG systems without the prior permission of the IT Department
- × **Don't** allow external contractors (or third parties) to gain access to CCG information systems without a contract in place ensuring compliance with appropriate CCG security policies
- × **Don't** interfere with antivirus software installed on CCG systems or purposefully upload or transmit a known computer virus or item of malicious software to others

Keeping Information Safe

The CCG 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.

Acceptable Use of IT Obligations

The CCG Acceptable Use of IT policy provides guidance on the acceptable use of CCG corporate IT hardware and software. Key messages to be aware of are:

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 CCG policies
- ✓ **Do** be aware that the CCG 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 in the Acceptable Use of IT policy
- ✓ **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 CCG network drive or systems for the installation of games or to store personal music or photographs. The CCG monitors its network drives and systems
- × **Don't** illegally duplicate copyrighted content onto CCG 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 the CGG to investigate and learn from them.

All Information Governance **Incidents** must be reported immediately to: IG Manager via datix **https://buryccg.datix.thirdparty.nhs.uk/live/index.php**

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

Unauthorised or accidental disclosure of, or access to personal data; unauthorised or accidental loss of access to, or destruction of, personal data; and unauthorised or accidental alteration of personal data. It is important that all incidents/near misses are reported within 24 hours of becoming aware of the incident.

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 Senior Information Risk Owner (SIRO) and Caldicott Guardian must be informed of such incidents, as appropriate, to enable an investigation to be carried out. This will be done by the IG Manager once the incident has been received through the reporting system There may be extra reporting mechanisms that the CCG 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 and also reported on Datix (**https://buryccg.datix.thirdparty.nhs.uk/live/index.php**). Your Line Manager is responsible for ensuring that all relevant people within the CCG have been informed of the incident.

Information Governance requirements for New Processes, Services and Systems

The CCG 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 IG 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. The IG Manager / Lead can support on advice if a DPIA is needed and assist in completion. 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 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

The CCG has adopted an Agile Working Policy.

The fundamental principle of our Agile Working model is that **work is something you do, not somewhere you go**. This increased flexibility, underpinned by a clear policy and focus on service delivery will support a continued reduced occupancy in offices. What this means is that as staff are working away from an office environment, there could be potentially be an increase in relation to unauthorised disclosure of information. It is important therefore that you follow the Information Security Policy and consider the risks associated with where you are working. For example, bear in mind discussions and/or meetings that you are involved in if you are in a public setting (such as a coffee shop) as confidential discussions should not take place in a public place and your laptop may be overlooked or in view by others. You should also ensure that you do not leave any equipment unattended.

DOs

✓ **Do** ensure any equipment supplied by the CCG is used only by you for CCG business

✓ **Do** ensure that Remote Access Service (RAS also known as VPN) Tokens are stored securely

✓ **Do** ensure passwords are not written down or shared with colleagues

✓ **Do** ensure you back-up and save work undertaken to CCG systems as soon as you return to the office

✓ **Do** take care when leaving public 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 NHS equipment or portable devices on display in your car, ensure they are locked away in your glove box or 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

- **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 where you may be overheard

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 CCG 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 CCG office environment. Ensure you apply suitable transportation methods so that information cannot be overlooked 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

As well as person-identifiable information the CCG 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 Social care

Staff must also adhere to the rules laid out in the
'A Guide to Confidentiality in Health and Social Care' – Health and Social Care Information Centre

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 Understand and Comply with the law

Principle 7 The duty to share information can be as important as the duty to protect patient confidentiality

Information Sharing

Person-identifiable information sometimes needs to be shared with other NHS 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 IG team.

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

The CCG have Secure Transfer of Information Guidance for flows of confidential information which must follow the Caldicott Principles. The CCG 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.

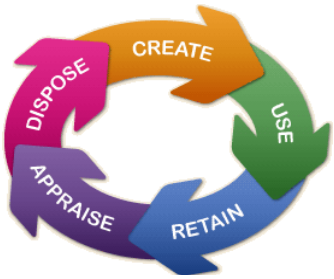
All routine transfers/flows of person-identifiable, confidential and sensitive information should

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 facsimile (fax), e-mail, post or other means.
Any members of staff handling confidential information, whether paper based or electronic must adhere to the Secure Transfer of Information Guidance.

Records Management

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



Records management is crucial to the CCG; 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, faxes, 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 the CCGs Records Management Policy.

It is important that staff do not store records on their PC Hard Drive. Records must be stored in the CCG shared drive/network in appropriate departmental electronic folders.

See the CCG 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 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 CCG system. We have to keep personal and public information accurate and up to date to comply with the Data Protection Act 2018.

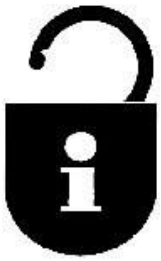
Data Protection

The CCG needs to process personal data about people in order to operate. These include current, past and prospective patients (this applies to specific services within the CCG for example Continuing HealthCare Department), 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 the CCG, this is known as a Subject Access Request. Details on how to request information can be found in the Privacy Notice on the Internet (www.buryccg.nhs.uk/We're here to help/Protecting your information/Accessing your information). This notice provides details of what personal information we collect and how it is used.

The CCG 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 UK (post Brexit) or European Economic Area (EEA) without adequate protection



DOs

- ✓ **Do** understand and comply with the eight DPA principles
- ✓ **Do** observe all CCG 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** delay – upon receipt of a Subject Access Request from an individual for information held about them, immediately notify CCG Information Governance Lead.
- ✗ **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 the CCG 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 the CCG 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:

CCG, Patient Services Department

Email: buccg.burypatientservices@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 Patient Services & Resilience 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 CCG please make sure that, as an absolute priority, you complete the e-learning Introduction to Information Governance & Data Security Mandatory Training Module via the Oracle Learning Management system (OLM). People Services at GMSS manage this system and will be able to assist you in accessing the system.

For existing staff and also in compliance to NHS digital data security & protection toolkit it is important that you keep up to date with best practice and changes in the legislation, therefore, each year you will need to update your Information Governance knowledge via the e-learning Mandatory Refresher Module provided by IBM via it's oracle learning management (OLM) system which is integrated in ESR.

You should also be aware the CCG has produced a Training Needs Analysis which has been drafted with support from IG manager. The Training Needs Analysis may require that depending on your job role and IG responsibilities within the CCG you may have to complete additional training.

Contact Details for People Services:
Email: **hr.businessservices@nhs.net**

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 ena bling appropriate information sharing.
CSUs	Commissioning Support Units
DPA	Data Protection Act
EEA	European Economic Area
EIR	Environmental Information Regulations
FOI	Freedom of Information
GMSS	Greater Manchester Shared Service
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
PCD	Personal Confidential Data
DPIA	Data Protection Impact Assessment
SIRO	Senior Information Risk Owner
SAR	Subject Access Request

IG Contact List

IG Team		
CCG IG Manager	Chidi Orisakwe	chidi.orisakwe@nhs.net

Information Governance Policies and 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 the CCG Information Governance policies, procedures, guidance, e-learning and useful contacts. All the documents can be found on the CCGs website.

Policy/Procedure Name
Information Governance Policy
Information Security Policy
Data Protection and Confidentiality Policy
Acceptable Use of IT Policy
Records Management Policy
Information Risk Policy
IG Incident Reporting Procedure
Confidentiality Audit Procedure
Confidentiality Code of Conduct
Confidentiality Agreement for Third Parties
DPIA Procedure and Template
Secure Transfer of Data
Subject Access Request Procedure

Your Information Governance Declaration

All CCG 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 Information Governance team - we are here to help you.

This Information Governance Handbook has been developed to ensure that CCG 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
- NHS Care Records Guarantee
- Human Rights Act (1998)
- Information Security Standard ISO27001
- Computer Misuse Act (1990)

Please remember that your computer and any CCG System login has been assigned to you only. As such, you are accountable for your computer and/or CCG 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** to 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 CCG 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 CCG disciplinary procedures.