Information Governance Staff Code of Conduct

July 2018

This Guidance has been developed by NHS Midlands & Lancashire Commissioning Support Unit (CSU), who act as NHS St Helens CCG's Information Governance Support Provider.

This Guidance has been approved and adopted by NHS St Helens CCG and is applicable to all staff, including contractors and volunteers.

Table of Contents

Consultation and Ratification Schedule	
Document Name:	Information Governance Staff Code of Conduct
Policy Number/Version:	1.0
Name of originator/author:	Midlands & Lancashire CSU Information Governance Team
Ratified by:	Finance, Governance and Risk Committee
Name of responsible committee:	Finance, Governance and Risk Committee
Date issued:	25.07.18
Review date:	June 2021
Date of first issue:	25.07.18
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of NHS St Helens CCG.
Purpose:	To outline the standards and expectation of staffs' compliance and expected code of conduct of all staff working for NHS St Helens CCG.
Action required:	All staff are required to read and sign the declaration at the back of the Staff Code of Conduct. Signing the declaration does not confirm that you are aware of everything but confirms that you have read it and know where to refer back to in the future if required.
Cross Reference:	Information Governance Handbook/Information Governance & Data Security and Protection Policies
Contact Details (for further information)	Midlands and Lancashire CSU Information Governance Team mlcsu.ig@nhs.net / 01782 872648

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version posted on the NHS St Helens CCG internet site is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Version Control

Information Governance Code of Conduct			
Version	Valid From	Valid To	Document Path/Name
0.1	05/06/2018	25/06/2018	Initial document

Glossary of Terms

Term	Acronym	Definition
Anonymisation		It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Business Continuity Plans	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable defined level.
Caldicott Guardian	CG	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
CareCERT		NHS Digital has developed a Care Computer Emergency Response Team (**CareCERT**). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.
Clinical Commissioning Group	CCG	They are responsible for commissioning healthcare services in both community and hospital settings.
Commissioning Support Unit	CSU	A Commissioning Support Unit (CSU) is an Organisation. Commissioning Support Units provide Clinical Commissioning Groups with external support, specialist skills and knowledge to support them in their role as commissioners, for example by providing: Business intelligence services.
Code of Conduct		A set of rules to guide behaviour and decisions in a specified situation.
Continuing Healthcare	CHC	CHC is health care provided over an extended period of time for people with long-term needs or disability / people's care needs after hospital treatment has finished.
Common Law		The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Care Quality Commission	CQC	This is an organisation funded by the Government to check all hospitals in England to make sure they are meeting government standards and to share their findings with the public.

Term	Acronym	Definition
Data Controller		The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor		A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Act 1998	DPA 1998	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.
Data Protection Act 2018	DPA18	Act replaced DPA 1998 above.
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with GDPR requirements.
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation.
Data Security and Protection Toolkit	DSP Toolkit	From April 2018, the DSP Toolkit will replace the Information Governance (IG) Toolkit as the standard for cyber and data security for healthcare organisations.
Data Sharing Agreement		A legal contract outlining the information that parties agree to share and the terms under which the sharing will take place.
Department of Health and Social Care	DOHSC	A department of the Government, responsible for government policy on health and adult social care matters in England.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities
General Data Protection Regulation	GDPR	The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’.

Term	Acronym	Definition
Information Assets		Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications.
Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Individual Funding Requests	IFR	Application to fund treatment or service not routinely offered by NHS.
Key Performance Indicators	KPI's	Targets which performance can be tracked against.
Pseudonymisation		The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Record Lifecycle		Records life-cycle in records management refers to the stages of a records "life span": from its creation to its preservation (in an archives) or disposal.
Senior Information Risk Owner	SIRO	Board member with overall responsibility for: • The Information Governance & Data Security and Protection Policies • Providing independent senior board-level accountability and assurance that information risks are addressed • Ensuring that information risks are treated as a priority for business outcomes • Playing a vital role in getting the institution to recognise the value of its information, enabling its optimal effective use.
Subject Access Request	SAR	A subject access request (SAR) is simply a written request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act.

Introduction

This code of conduct sets out clear guidance and the Information Governance standards expected of staff working for NHS St Helens CCG.

All employees working in the CCG, including temporary staff such as all contractors, voluntary staff, and students are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work.

This is not just a requirement of your contractual responsibilities but also a requirement within the new Data Protection Act (see legislation below), the Common Law Duty of Confidentiality and the NHS Confidentiality Code of Practice 2003 and any other appropriate professional codes of conduct.

This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should be also be treated with the same degree of care e.g. business in confidence information such as patient referral letters, discharge summaries, waiting list data, workloads and clinic lists.

Disclosure and sharing of personal identifiable information is governed by the requirements of Acts of Parliament and the Common Law Duty of Confidentiality. There are exceptions where it is sufficiently in the public interest to warrant a breach of disclosure, for example in relation to a serious crime or in instances to prevent serious harm or abuse.

Legislation

From May 2018, the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR) and will be referred to as Data Protection Act 2018 or GDPR/DPA18. The core principles will remain, however GDPR/DPA18 is more stringent about when we can use personal data, what we need to tell individuals about what we hold, how we use personal data and how quickly we need to respond in the event of a personal data breach.

The GDPR/DPA18 also requires us to demonstrate how we comply with the Regulation and introduces stricter fines for non-compliance - up to 4% of an organisations total income or 20 million euros, whichever is greater.

Principles of GDPR/DPA18

- **Lawful, fair and transparent processing** – this principle emphasises transparency for all EU data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the Data Protection Officer is at that organisation or what data the organisation has about them, that information needs to be available.

- **Purpose limitation** – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Consider all the organisations that require forms with 20 fields, when all they really need is a name, email, shipping address and maybe a phone number. (Simply put, this principle says that organisations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do can be out of compliance).

- **Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant and limited. In this day and age, businesses collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviors and patterns or remarketing based on intelligent analytics. Based on this principle, organisations must be sure that they are only storing the minimum amount of data required for their purpose

- **Accurate and up-to-date processing** – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work, but a conscious effort to maintain accurate customer and employee databases will help prove compliance and also prove useful to the business.

- **Limitation of storage in the form that permits identification** – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organisations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is a compliance nightmare.

- **Integrity, Confidential and Secure** – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting, and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects. Negligence is no longer an excuse under GDPR, so organisations must spend an adequate amount of resources to protect the data from those who are negligent or malicious. To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilising dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware.

GDPR also introduces the principle of accountability:

- **Accountability and liability** – this principle ensures that organisations can demonstrate compliance. Organisations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organisations must be sure that every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, GDPR requires organisations to respond to requests from data subjects regarding what data is available about them. The organisation must be able to promptly remove that data, if desired. Organisations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.

Caldicott Principles

In addition to the GDPR/DPA18 principles above staff working in the NHS handling patient information, whether you are requesting, using or disclosing confidential patient information should, at all times, be aware of and comply with the Caldicott Principles below, these are:

1. **Justify the purpose of using confidential information.** Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined.

2. **Only use it when absolutely necessary.** Patient-identifiable information should not be used unless there is no alternative.

3. **Use the minimum necessary personal confidential data**. Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

4. **Access should be on a strict need-to-know basis**. Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see

5. **Everyone must understand their responsibilities.** All those who handle patient-identifiable information should be made aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law**. Every use of patient-identifiable information must be lawful. Every NHS organisation should have someone responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality.** Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

If you have any concerns about disclosing/sharing patient/staff information you must discuss this with your manager in the first instance or, if you are uncertain whether disclosure of information can take place, contact the Caldicott Guardian/Information Governance team.

The Common Law Duty of Confidentiality

All staff working for the CCG also have a common law duty of confidentiality.

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

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

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is in the public interest; and
- where there is a legal duty to do so, for example a court order.

Therefore, under the common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. Solid justification is required before individual rights are set aside, and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.

If a disclosure is made which is not permitted under common law the patient can bring a legal action not only against the organisation but also against the individual responsible for the breach

Information Governance

NHS St Helens CCG has an Information Governance Policy which sets out at a high level how we comply with the GDPR/DPA18. All staff are responsible for complying with the CCG Information Governance & Data Security and Protection Policies. Service and Heads of departments are responsible for ensuring that staff follow CCG policies, processes and guidance. In practice, this means managers should make staff aware of such documents and, where appropriate, advise staff where those processes should be followed.

NHS St Helens CCG contract Midlands and Lancashire CSU to provide a team of Information Governance specialists to help all staff to comply with their Information Governance responsibilities. Specifically, the team will support staff through designing training, policies and guidance and offering specialist advice to staff in their respective areas.

Information Governance Training

Information Governance knowledge and awareness is at the core of the organisations objectives, without this the ability of the organisation to meet legal and policy requirements will be severely impaired.

To ensure organisational compliance with the law and central guidelines relating to Information Governance **all staff are mandated to complete annual IG training**.

Collecting and Using Personal Data

Data Minimisation:

- Consider whether you need personal data to achieve your objective.
- Only collect or use the minimum amount of personal data needed for your specific business objective.

Transparency

- Ensure individuals have been given information about how and why we use their personal data, how long we hold onto their data, who we share it with, the CCG's responsibilities under the DPA18 and their rights in relation to their data under that Act ('the fair processing information').

Internal Disclosure

- Only share personal data with other teams where those teams have a genuine business need to access the personal data.
- Only share the minimum amount of personal data with those teams who need to deliver their business objective.
- If you are using the data for an entirely new purpose, you should also complete Data Privacy Impact Assessment (DPIA) screening questions on UAssure to identify whether a Data Privacy Impact Assessment (DPIA) should be undertaken.

External Disclosures

- Staff may receive a broad range of requests from external organisations to disclose personal data, such requests should be passed to the SARs Team who will co-ordinate the disclosure.

Information Governance Data Breaches/Incidents

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data means information in any form including paper records, emails, faxes etc. Examples of personal data breaches can include, forwarding a spreadsheet of patient data to an unintended recipient (external or internal) or a theft of sensitive documents left in an unlocked room.

Personal data breaches must be reported as soon as possible following the incident.

- If you know or suspect a personal data breach/incident may have occurred complete an incident form or contact a member of the IG Team

- The IG team member will ask you for detail about the circumstances of the breach, the type of data involved and, who that data relates too and potential impact on individuals affected.
- From May 2018 under GDPR/DPA18, NHS St Helens CCG will be subject to a strict 72-hour timescale in which to report such breaches to the regulator, the Information Commissioner Office. The CCG could be subject to a substantial fine for failure to report within this period.
- **It is important to remember that the 72-hour timeframe starts from the moment any individual in the organisation discovers that a personal data breach has occurred.**

Abuse of Privilege

Staff must not abuse their position by viewing any information regarding 'VIPs or celebrities', unless they are directly involved in their care. Staff must not disclose the fact that anyone famous or not is using CCG services.

It is strictly forbidden for employees to look at any information relating to their own family, friends, work colleagues or acquaintances unless they are directly involved in the patient's clinical care or with the employee's administration (e.g. payroll) on behalf of the CCG.

Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

If you have concerns about this issue, please discuss with your line manager.

Social Networks and Blogs

Social Networking site, such as Facebook, Twitter and Instagram, are a very popular way for people to communicate with one another.

What is important to bear in mind is that what you post online is in the public domain. Even if you have made your profile only viewable to friends, what you write can still be seen by others. So, a tirade which may seem harmless to you, might be interpreted differently by others.

Here are some considerations you may wish to apply when using these sites. It is important to remember particularly in the NHS - patient confidentiality is essential!

A Guide to help make sure you do not inadvertently break the law, or breach NHS St Helens CCG policies:

- Do not make disparaging or inappropriate comments about the CCG, its patients or your colleagues on a social networking site.
- Never identify patients in your care, or post information that may identify a patient
- If you use sites like Facebook, Instagram or Twitter, do make sure that only friends and people you know can see your information. You can also stop your profile or information from appearing on search engines like Google. This way not everyone is going to be able to read what you post.
- If you are a qualified healthcare professional, do read the requirements and/or guidance laid down by your professional body e.g. NMC, GMC etc.
- If you are required to take photographs or use a video for work purposes, ensure you have permission and do not include any personal identifiable information. These must not be uploaded onto any social media sites. Inappropriate postings on social networks which are detrimental to other employees or could bring the CCG into disrepute may result in disciplinary action being taken.

Carelessness

- Do not talk about patients/staff in public places or where you can be overheard.
- Do not leave any medical records or confidential information, including diaries, unattended.
- Make sure that any computer screens, or other displays of information, cannot be seen by the general public.

Internal and External Mail

Best practice with regards to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient.

This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team Leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate.

External Mail must also observe these rules. Special care should be taken with personal information sent, such as patient records on paper, disc or other media. These should be sent by courier or by recorded/registered post, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. copy of patient records sent to a solicitor.

Generally, mail is franked with a return address, but in instances where this does not occur, ensure that a return address is printed on the outside of the envelope to prevent post being inappropriately opened where addresses are incorrect

Fax

Fax machines must only be used to transfer confidential information when it is absolutely necessary to do so. The following rules must apply: -

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it
- The sender is certain that the correct person will receive it and that the fax number is correct
- You notify the recipient when you are sending the fax and ask them to telephone that the whole fax has been properly received
- Care is taken in dialing the correct number
- Confidential faxes are not left unattended for unauthorised staff to see
- Only the minimum amount of personal information should be sent. Where possible the data should be anonymised or a unique identifier used e.g. NHS Number
- Use a fax cover sheet that includes:
    - Who the fax is from
    - The name of the recipient
    - The number of pages the fax contains (including the top copy)
    - Notification of the recipient to contact the sender on the arrival of a fax
    - A suitable confidentiality clause

Storing confidential information

Paper-based confidential information should always be kept in a secure environment and preferably in a room that is locked, when unattended, particularly at nights and weekends or when the building/office is not occupied for a long period of time.

Electronically held confidential information must not be saved onto local hard drives, but onto secure network drives. Where confidential information has to be stored on removable media e.g. USB memory sticks, then it must be encrypted in line with the minimum DoHSC standards. For further details please contact the Information Governance team or the IT Service Desk.

When information is saved to a network drive then access to that information must be on a strict 'need to know 'basis.

Disposal/destruction of Confidential Information

When disposing of paper-based confidential information always use confidential waste bins provided. Keep the waste in a secure place until it can be collected for secure disposal.

Removable media containing confidential information must be reformatted or securely destroyed; this can be arranged by contacting the IT Service Desk.

Computer hard disks must be destroyed or disposed of by the IT department.

Mobile working

NHS St Helens CCG understands that staff are often required to work away from their usual work locations, for this reason the following principles have been developed which must be adhered to at all times:

- No person identifiable or commercially sensitive information should be worked on remotely unless connected securely via the Virtual Private Network (VPN).
- Users should connect to the network via the organisations VPN. A VPN is a computer network that uses the Internet to provide individual users with secure access to their organisations network. The VPN provides a secure communication between organisations owned hardware (i.e. laptops) connected to non-NHS networks and the organisations network. The capability to utilise VPN is automatically included in the build of all the organisations laptops and is comparable to utilising a PC to access information, therefore authorisation to use this facility is not required beyond the initial authorisation for the purchase/use of the laptop.
- No information should be saved to the hard drive of a laptop, to a USB stick or to any other removable media for the purpose of remote working. This is not an authorised procedure and this practice should cease with immediate effect.
- Emailing work as attachments to either personal accounts or work account is not an approved method of working remotely and must not take place.
- Accessing information belonging to the organisation in public accessible areas is discouraged, due to the threats of “overlooking” and theft of equipment. Staff are responsible for ensuring that unauthorised individuals are not able to see information or access systems.
- Computer equipment should never be left unattended when logged in and switched on and must be securely locked away when not in use.
- Records and equipment must always be transported in a secure way e.g. in a sealed container, briefcase, kept in the boot of the car and not visible to the general public. Records must be securely locked as soon as practicable and should not be left in the boot of the car overnight.
- If physical records are taken from their base location to enable mobile working, they should be tracked to ensure their location can be identified.

Home working

It is sometimes necessary for employees to work from their own home. If you need to do this, you first need to gain approval from your line manager. If they agree you then need to ensure the following are considered and remember that there is personal liability under the law and your contract of employment for breach of these requirements:

Ensure you have authority to take any records away. This will normally be granted by your line manager.

- If you are taking manual records please ensure there is a record that you have these records, where you are taking them to, the purpose for taking them and when they will be returned. This is particularly important for records that may contain sensitive data, for example patient/staff records.
- Make sure when travelling home that they are put in the boot of the car out of sight (ensuring that the vehicle is locked when unoccupied) or carried on your person while being transported from your work place to your home.
- While at home you have personal responsibility to ensure the records are kept secure and

confidential. This means that other members of your family and/or your friends/colleagues must not be able to see the content or outside folder of the records.

- You must not let anyone have any access to the records.
- When returning the records to work the same procedure must be carried out, as above.
- Laptops containing personal identifiable information must be secured at all times, especially in transit.
- Any loss of records or data bearing media, such as laptops, must be reported immediately to your line manager as soon as the loss is known.
- If appropriate the police should also be informed.

Subject Access Requests (Access to Personal Information)

Every living person (or their authorised representative) has the right to access information/records held about them by an organisation.

The record can be in manual (paper files) or in computerised form and may include such documentation as hand written notes, letters, reports, imaging records, photographs, DVD and sound recordings.

Under GDPR/DPA18 information requested must be provided without delay and at the latest within **one month** of receipt.

Failure to comply and provide information requested under GDPR could result in a substantial fine.

The maximum fine that can be issued by the Information Commissioner Office (ICO) is 4% of an organisations global turnover or 20 million euros, whichever is higher. Individuals also retain the right to pursue a claim in court.

A SAR must be made in writing; however, the requestor does not need to mention the GDPR/DPA18 or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 1998, but their request should still be treated according to this policy.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Fax
- Post
- Social media
- CCG website

Requests for information held about an individual must be directed immediately to the SAR team.

Freedom of Information

The Freedom of Information Act (2000) came into effect for all public authorities in January 2005. Since then, all requests for information have had to be answered in accordance with the Freedom of Information (FOI) Act 2000 or the Environmental Information Regulations 2004 (EIR).

The Freedom of Information Act gives a general right of access to all types of recorded information held by public authorities, if you are unsure about a request for information contact the FOI team in the first instance.

A request for information under the general rights of access must be:

- received in writing
- state the name of the applicant and an address for correspondence
- clearly describe the information requested
- a request can also be made electronically via email.

The deadline for a public authority to respond to requests made under the Act is **20 working days, it is therefore vital that all requests are forwarded to the FOI team immediately.**

Information Security

Data stored electronically in CCG information systems is critical to patient care and vital to the smooth running of the organisation.

It is essential that each of us play our part in protecting the confidentiality, integrity and security of our information.

Everyone who works for the CCG has responsibility for protecting the security of our systems.

Failure to comply with the guidance contained in this document may lead to disciplinary action.

Your Passwords

You will have been provided with passwords to enable you to access systems.

Always keep your passwords secure by:

- Never writing them down
- Never sharing them with others
- Changing them regularly

If you suspect that any of your passwords have become known to any other person or if you lose your Smartcard, you must report this immediately to the IT Service Desk.

Keeping our Computers Secure

The security of our equipment is one of the keys to the safety of our information.

- When you leave your computer unattended, even for a short while, always lock it and / or remove your Smartcard
- You can lock your computer by pressing the **Ctrl, Alt and Delete** keys together and then selecting '**Lock Computer'**
- Take extra care to keep mobile devices secure at all times. Never leave them unattended in a public place or unsecured office. Data must only be stored on laptops or memory sticks provided by the CCG (as these are suitably encrypted) unless an exception has been approved in writing by the Senior Information Risk Owner (SIRO).
- Devices that are not supplied by the CCG must not be used to access computers or networks without authorisation from the IT Department
- Never install any software not provided by the CCG onto its systems unless approved by the IT Department
- Do not allow anyone who doesn't work for the CCG to use our equipment unless approved by the SIRO.

Smartcards

Your Smartcard provides you with the level of access to information you require as part of your role. Smartcards are issued to individual members of staff and must only be used by the person whose name is on the card.

Accessing information using another person's Smartcard is against the law, even if you are authorised to have access to the information. Users of Smartcards must follow the terms and conditions of use – these can be found on the Smartcard application form (RA01).

Care must be taken by everyone issued with a Smartcard to keep it secure and protect their pin against discovery, and cards should be treated with care and protected to prevent any loss or damage.

Using Electronic Mail

Most of us use email to communicate with our colleagues. This makes communication very easy and quick but there are risks and you need to be aware of how to ensure that your messages remain secure:

- Only use the email system supported by the CCG – NHS.net (NHSmail)
- Always re-read your message before sending, checking that it is addressed to the correct person
- If you are unsure of where a message has come from or if it contains an unexpected attachment, do not open it and contact the IT Service Desk for advice
- Be aware of the dangers of hoax emails and those that request personal details. Always report these to the IT Service Desk
- Never respond to an email asking for a password
- Never send material that is discriminatory, sexist or contains offensive material (including joke emails)
- Do not write something in an email that you would not write in a letter - email has the same legal status

Whilst we have all experienced the speed of email, it is not always an instant communication and you should not assume that sent messages are received without further confirmation from the recipient. This is particularly important when sending urgent messages or those with large or unusual attachments.

Emailing Personal Confidential Data (PCD)

You should be particularly careful when emailing PCD.

As noted above, emailing from a nhs.net email address to another nhs.net address is secure.

Confidential information or data must never be transmitted over the internet unless the data is encrypted.

Using the Internet

For many of us, the Internet is regularly used to provide a key source of information to help us in our daily work. However, it is important to follow some rules to ensure that our information remains safe and secure:

- When using the Internet, programs may be automatically downloaded and run. If you are concerned about the way a program is behaving, contact the IT Service Desk for advice
- Ensure that any material that you download complies with any copyright restrictions and does not contain discriminatory, sexist or offensive material
- Don’t assume that all information found on the Internet is necessarily accurate or up to date
- If you are using a password protected application over the Internet always ensure that you are accessing a secure Internet site

Personal Use and Social Networking

The CCG accepts that staff may, on occasions, need to deal with pressing personal tasks during working hours and therefore a limited amount of personal use of email and access to the Internet is permitted.

You should ensure that you are familiar with the policy on personal use and adhere to the published guidance at all times. Specifically:

- You should not use this facility for any outside commercial or business activity
- You should not engage in extensive social activities such as chat rooms, gaming, blogging or auctions
- Personal use of social networking sites should be kept to a minimum and accessed only outside of your working hours

Whenever and wherever you engage in computer activity, including outside the CCG you must NOT:

- Reveal confidential information about patients, staff or the CCG
- Attack or abuse colleagues
- Use defamatory, derogatory or offensive comments especially about colleagues, staff or patients
- Engage in activities that might bring the CCG into disrepute

Specialist Applications

You may be using specialist software applications within your work area, in which case you should comply with all specific training and documentation that will have been provided to you.

We need to know where data is stored throughout the CCG and therefore you must not set up any independent databases or spreadsheets containing Personal Confidential Data without first consulting the Information Governance department or your Line Manager.

Monitoring Computer Activity

You should be aware that the CCG actively monitors all computer activity to maintain the effective operation of the systems and to comply with any legal obligations.

Electronic documentation and records of activity may be disclosed if required by law.

Virus Protection

Whilst virus protection software is in operation, you can help to prevent an infection by:

- Immediately deleting any spam or chain emails without opening them
- Not opening or forwarding emails or files from unknown sources
- Not opening unexpected attachments received by email

If you suspect that your computer has been infected with a virus, have any doubts about an email attachment or experience unusual system behavior, you should contact the IT Service Desk for advice.

For more help or for any further questions please contact the Information Governance Team.

Code of Conduct Sign Off Form

Acknowledgement of your personal responsibility concerning the security and confidentiality of information relating to patients, staff and the organisation:

Personal Details	
Surname	
Forename(s)	
Job Title	
Department	
Location	

Declaration:

I can confirm that I have read and acknowledge the content of the NHS St Helens CCG Information Governance Staff Code of Conduct.

I understand that I am bound by a duty of confidentiality and agree to adhere to the Code of Conduct at all times.

Signature: ……..

Date: ……..