Information Governance Staff Code of Conduct

NHS Lancashire & South Cumbria Integrated Care Board

V3.0

Contents

Consultation and Ratification Schedule

Consultation and Ratification Schedule	
Document Name:	Information Governance Staff Code of Conduct
Policy Number/Version:	3.0
Name of originator/author:	NHS ML Information Governance Team,
Ratified by:	NHS Lancashire and South Cumbria Integrated Care Board
Name of responsible committee:	Lancashire and South Cumbria Integrated Care Board Audit Committee
Date of first issue and where published:	1st July 2022 (website)
Date of current issue	19th December 2024 (minor amends 1 September 2026)
Review date	19th December 2026
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of: NHS LANCASHIRE & SOUTH CUMBRIA INTEGRATED CARE BOARD
Purpose:	To outline the standards and expectation of staffs' compliance and expected code of conduct of all staff working for: NHS LANCASHIRE & SOUTH CUMBRIA INTEGRATED CARE BOARD
Action required:	All staff are required to read and sign an electronic declaration at the end 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 to in the future if required.
Cross Reference:	Information Governance Handbook Information Governance & Data Security and Protection Policies Anti-Virus Policy IT Acceptable Use Policy Asset Management Policy IT Encryption Policy IT Vulnerability Management Policy Network Security Policy User Account Management Policy Password Management Policy
Contact details and further information:	• Email: infogov.lscicb@miaa.nhs.uk • Service Desk Contact Number: 0330 236 6965

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Integrated Care Board's 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**
1.0	01/07/2022	30/09/2024	Full review for new Integrated Care Board organisation
2.0	18/12/2024	18/12/2024	Full review
2.1	28/08/2026	28/08/2026	Updated service provider and contact details throughout.

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.
Commissioning Support Unit	CSU	A Commissioning Support Unit (CSU) is an Organisation. Commissioning Support Units provide Integrated Care Boards 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	CoC	A set of rules to guide behaviours 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, Primary Care, and other health and care providers in England are meeting government standards and to share their findings with the public.
Corporate Records		Records which relate to the corporate business of the Integrated Care Board such as accounts, minutes and meeting papers and legal and other administrative documents. They may contain personal identifiable information, for example personnel files and should be treated with the same degree of care and security as patient/service user records.

Data Controller	DC	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	DP	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Processing Agreement	DPA	A legally binding agreement outlining the responsibilities of the Data Controller and the Data Processor when a Data Processor is appointed on behalf of a Data Controller.
Data Protection Act 2018	DPA18	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 Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with UK 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	DSPT or DSP Toolkit	The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations that have access to NHS patient data and systems to provide assurance that they are practising good data security, and that personal data is handled correctly.
Data Subject		An identified or identifiable living individual to whom personal data relates.
Data Sharing Agreement	DSA	A non-legally binding agreement outlining the information that Data Controllers agree to share and the terms under which the sharing will take place.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities
Health Records		Records which consist of information relating to the physical or mental health of an individual and has been made by or on behalf of a health professional in connection with that care.

Information Asset Administrator	IAA	Information Asset Administrators work with the IAOs to implement the Information Risk Work Programme, updating the information asset registers and data flow mapping and ensuring policies are being properly adhered to.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own.'
Information Assets		Includes records and documents that contain key information to the organisation's business.
Information Commissioner Office	ICO	The Information Commissioner Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Integrated Care Board	ICB	A statutory NHS organisation responsible for developing a plan for meeting the health needs of the population, managing the NHS budget and arranging for the provision of health services in the Integrated Care System area.
Integrated Care Partnerships	ICP	A statutory committee jointly formed between the NHS Integrated Care Board and all upper-tier local authorities that fall within the Integrated Care System area. The Integrated Care Partnership will bring together a broad alliance of partners concerned with improving care, health and wellbeing of the population, with membership determined locally. The Integrated Care Partnership is responsible for producing an integrated care strategy on how to meet the health and wellbeing needs of the population in the Integrated Care Systems area.
Integrated Care Systems	ICS	Integrated Care Systems are partnerships of organisations that come together to plan and deliver joined up health and care services, and to improve the lives of people who live and work in their area.
Individual Funding Requests	IFR	Application to fund treatment or service not routinely offered by NHS.
Key Performance Indicators	KPIs	Targets which performance can be tracked against.
Mersey Internal Audit Agency	MIAA	The ICB's Information Governance service provider.

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.
Records		Recorded information in any form or medium, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs.
Record Lifecycle		A period a record exists from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as semi-active or closed records which may be referred to occasionally) and finally either confidential destruction or archival preservation.
Records Management		A discipline which utilises administrative systems to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound; whilst at the same time serving the operational needs of the Integrated Care Board and preserving an appropriate historical record.
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 or verbal 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.
United Kingdom General Data Protection Regulation	UK GDPR/GDPR	"GDPR" means UK GDPR. UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

Introduction

This code of conduct sets out clear guidance and the Information Governance standards expected of staff working for the Integrated Care Board.

All employees working in the Integrated Care Board, 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 encounter non-person identifiable information which should also be treated with the same degree of care.

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

The UK General Data Protection Regulation (UK GDPR) is a legal framework that follows the EU GDPR and sets guidelines for the collection and processing of personal information from individuals while the Data Protection Act 2018 sets out the data protection framework in the UK.

UK GDPR and DPA18 are 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 UK 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 organisation's total annual worldwide turnover in the preceding financial year or £17.5 million, whichever is greater.

Principles of UK GDPR/DPA18

- **Lawful, fair, and transparent processing** – this principle emphasises transparency for all 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 behaviours 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 not an excuse under UK GDPR, so organisations must spend an adequate number 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.

UK 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 UK GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, UK 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 UK 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 confidential information should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed by an appropriate guardian.

2. **Only use confidential information when absolutely necessary.** Patient-identifiable information should not be used unless there is no alternative. Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

3. **Use the minimum necessary personal confidential data.** Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

4. **Access to confidential information should be on a strict need-to-know basis.** Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

5. **Everyone with access to confidential information should be aware of their responsibilities.** Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patients and service users.

6. **Understand and comply with the law.** Every use of confidential information must be lawful. Every NHS organisation should have someone responsible for ensuring that the organisation complies with legal requirements. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

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

8. **Inform patients and service users about how their confidential information is used.** A range of steps should be taken to ensure no surprises for patients and

service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use of data. As a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.

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 Integrated Care Board 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.

The circumstances when disclosing confidential information lawfully are:

- where the individual to whom the information relates has consented,
- where disclosure is in the public interest and outweighs protecting confidentiality,
- where there is a statutory requirement or legal duty to do so, for example a court order; and,
- where there is approval under Section 251 of the NHS Act 2006 to use the data for indirect patient care purposes such as planning and research. For this support under Regulation 5 of the Control of Patient Information Regulation 2002 (COPI) approval is required from the Health Research Authority's (HRA) Confidentiality Advisory Group (CAG).

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.

Specialist or legal advice should also be sought where it is proposed to use patient data for secondary purposes and the duty of confidence needs to be set aside by way of a Confidentiality Advisory Group approval.

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

The Integrated Care Board has an Information Governance Policy which sets out at a high level how we comply with the UK GDPR/DPA18. All staff are responsible for complying with the Integrated Care Board's Information Governance & Data Security and Protection Policies. Service and Heads of departments are responsible for ensuring that staff follow the Integrated Care Board's 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.

The Integrated Care Board contracts Mersey Internal Audit Agency (MIAA) 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 Integrated Care Board'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 Protection Impact Assessment (DPIA) screening questions to identify whether a DPIA, or perhaps an assurance checklist, 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 mlcsusars@nhs.net 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, 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, please follow the Integrated Care Board's Breach Standard Operating Procedure (SOP) and contact a member of the Information Governance team - email: infogov.lscicb@miaa.nhs.uk Service Desk Contact Number: 0330 236 6965

- The Information Governance team member will ask you for details about the circumstances of the breach, the type of data involved, who that data relates to and the potential impact on individuals affected.

- The Integrated Care Board is subject to a strict 72-hour timescale in which to report such breaches to the regulator, the Information Commissioner's Office (ICO). The Integrated Care Board 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. The Information Governance team should be informed at the earliest opportunity in order to allow them to ascertain sufficient information.**

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 the Integrated Care Board's 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 Integrated Care Board.

Employees are also not allowed to view their own personal information. Should an employee wish to have a copy of their own information they should make a Subject Access Request (SAR).

Abuse of privilege 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 sites, such as Facebook, X (formerly 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 ensure you do not inadvertently break the law, or breach Integrated Care Board policies:

- Do not make disparaging or inappropriate comments about the Integrated Care Board, data subjects, 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 X, 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 patients or could bring the Integrated Care Board into disrepute and 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.

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 Department of Health and Social Care (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 Integrated Care Board’s IT provider.

Computer hard disks must be destroyed or disposed of by the Integrated Care Board’s IT provider.

Mobile Working

The Integrated Care Board understand 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 organisation’s VPN. A VPN is a computer network that uses the Internet to provide individual users with secure access to their organisation’s network. The VPN provides a secure communication between the organisation’s owned hardware (i.e., laptops) connected to non-NHS networks and the organisation’s network.

- No personal confidential 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 using a personal account is not an approved method of working remotely and must not take place.

- Accessing information belonging to the organisation in publicly 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 away 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

If agile working is a requirement for your job role, 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 workplace 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.

Working From Abroad

Staff members should not work from abroad without obtaining all necessary permissions – this includes (but may not be limited to) line managers, the Senior Information Risk Owner and the Caldicott Guardian at the Integrated Care Board. If you wish to make a request to work abroad, please liaise with the Information Governance Team who can facilitate and advise on a case-by-case basis.

Printing From Home

- Reduce paper-handling to zero, where possible. Only print documents if necessary.

The following questions need to be considered before deciding whether it is necessary to print from home:

- Is it something that urgently needs to be printed? Or can it be done electronically?
- Is this a benefit to you or an individual?
- If a benefit to you is there another approach you can take that completes the actions/tasks you are required to complete?
- Are you going to need IT provider assistance to connect your personal printer to your work device?
- Have you got access to your normal work base to print documents?
- Does the information contain personal information?
- Do you need to scan personal information back onto the system via your personal home printer?
- If you were unable to print information, would this impact individual patient care?
- If you do print from home, you need to follow strict protocols in relation to the storage and secure disposal of any confidential information. Data Protection requirements do not relax just because you are working remotely.
- Disposing of information that is not subject to records retention must follow strict guidelines.
- If you are shredding documents at home, your shredder must meet required standards of a DIN-4-Cross-Cut shredder which shreds documents into particles of at least 160mm, as per the DIN66399 standard developed by the Standards Committee for Information Technology and Applications.
- If it does not or in the absence of a shredder, you must discuss disposal of confidential waste with the IG Team.

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 handwritten notes, letters, reports, imaging records, photographs, DVD, and sound recordings.

Under UK 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 UK GDPR could result in a substantial fine.

The maximum fine that can be issued by the Information Commissioner's Office (ICO) is 4% of an organisation's global turnover or £17.5 million, whichever is higher. Individuals also retain the right to pursue a claim in court.

A Subject Access Request (SAR) can be made verbally or in writing; however, the requestor does not need to mention the UK 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 2000, but their request should still be treated according to this code of conduct.

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

- Email,
- Post,
- Social media,
- Integrated Care Board's website.

- Requests for information held about an individual must be directed immediately to mlcsusars@nhs.net.

Freedom of Information (FOI)

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 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 or made electronically (e.g. email)
- state the name of the applicant and an address for correspondence.
- clearly describe the information requested.

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 mlcsu.foi@nhs.net immediately.

Information Security

Data stored electronically in the Integrated Care Board's 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 Integrated Care Board has a 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 remove your Smartcard.

- You can lock your computer by pressing the **Ctrl, Alt and Delete** keys together and then selecting **'Lock Computer'** or by pressing the **Windows and L** keys together.

- 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 Integrated Care Board (as these are suitably encrypted) unless an exception has been approved in writing by the Senior Information Risk Owner.

- Devices that are not supplied by the Integrated Care Board must not be used to access computers or networks without authorisation from the Integrated Care Board's IT provider.

- Never install any software not provided by the Integrated Care Board onto its systems unless approved by the Integrated Care Board's IT provider.

- Do not allow anyone who doesn't work for the Integrated Care Board to use our equipment unless approved by the Senior Information Risk Owner.

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 Integrated Care Board – NHS.net (NHSmail).
- Always re-read your message before sending, checking that it is addressed to the correct person.
- Always check when using the 'reply all' function. Remove unnecessary content and attachments. Avoid forwarding entire emails, email trails and attachments, unless you have checked it for Personal Data, and it is necessary for recipients to see.
- 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 Integrated Care Board's IT provider for advice.
- Be aware of the dangers of hoax emails and those that request personal details. Always report these to the Integrated Care Board's IT provider.
- 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. If you are sending from an nhs.net account to a non nhs.net account, you should use the encryption facility as described within the Information Governance Handbook.

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

Email Phishing Attacks and Protection Against Them

A phishing attack aims to get users to do the wrong thing. This is done by using social engineering which is a term which means simply trying to convince an individual through use

of pressure, either pretending to be in a position of authority or that there is urgency in action being taken.

NHS Mail will automatically provide some protection against phishing attacks. It's important to remain vigilant and double-check email addresses from recipients to ensure they are legitimate. Look out for email address not in the expected format, e.g. firstname.lastname@nhs.net, a series of numbers/letters forming part of the email address or just an unexpected sender. If you receive what you believe to be a phishing attack, forward the email to spamreports@nhs.net and double delete it from your own inbox.

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 Integrated Care Board 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 Integrated Care Board you must NOT:

- Reveal confidential information about patients, staff, or the Integrated Care Board.

- Attack or abuse colleagues.
- Use defamatory, derogatory, or offensive comments especially about colleagues, staff, or patients.
- Engage in activities that might bring the Integrated Care Board 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 Integrated Care Board and therefore you must not set up any independent databases or spreadsheets containing Personal Confidential Data without first consulting the Information Governance team or your Line Manager.

Monitoring Computer Activity

You should be aware that the Integrated Care Board 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 behaviour, you should contact the Integrated Care Board's IT provider for advice.

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