

NHS Cheshire and Merseyside ICB

Information Governance Handbook

October 2022



Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

Contents

[Consultation and Ratification Schedule](#) 7

[Glossary of Terms](#) 8

[Information Governance – Top Do’s and Do Not’s](#) 13

[General Do’s and Do not’s](#) 13

[Do’s](#) 13

[Do Not](#) 14

[Information Governance Handbook](#)..... 14

1.0 [Introduction](#) 14

2.0 [Legislation and Regulations](#) 15

3.0 [Principles of the UK General Data Protection Regulation/Data Protection Act 2018:](#) 15

4.0 [Appointment of Data Protection Officer](#) 16

5.0 [Caldicott Guardian Principles](#) 16

6.0 [Confidentiality](#)..... 17

7.0 [Summary of key roles and responsibilities](#) 17

 7.1 [Senior Information Risk Owner](#) 17

 7.2 [Information Asset Owners](#) 17

 7.3 [Information Asset Assistants](#) 18

 7.4 [Caldicott Guardian](#) 18

 7.5 [Data Protection Officer](#) 18

 7.6 [Information Governance Team](#) 18

8.0 [Secure Working Environment - Premises security & Off-Site Working](#) 18

 8.1 [ID Badges](#) 18

 8.2 [Access Control](#)..... 19

 8.3 [Printing From Home](#) 20

 8.5 [Clear Screen & Clear Work Area](#) 20

[Clear Screen](#)..... 20

[Clear Work Area](#) 21

9.0 [Information Governance Induction for New Starters](#)..... 21

10.0 [Annual Information Governance Training](#)..... 22

11.0 [Individual’s Rights](#) 222

 11.1 [The right to be informed](#)..... 22

Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

- 11.2 [The right of access](#) 22
- 11.3 [The right to rectification](#) 222
- 11.4 [The right to erasure](#) 233
- 11.5 [The right to restrict processing](#)..... 244
- 11.6 [The right to data portability](#) 255
- 11.7 [The right to object](#)..... 25
- 11.8 [Rights in relation to automated decision making and profiling](#) 266
- 11.9 [The right to withdraw consent](#)..... 266
- 12.0 [Subject Access Requests](#)..... 27
 - 12.1 [Access to Information \(Subject Access Requests -SAR\)](#)..... 27
 - [Timescales to respond to a SAR](#) 27
 - [Fees](#)..... 277
 - [Failures to meet requests for information](#) 277
 - 12.2 [Recognising a SAR](#)..... 27
 - 12.3 [SAR Flowchart](#)..... **Error! Bookmark not defined.**
- 13.0 [Freedom of Information \(FOI\)](#)..... **Error! Bookmark not defined.**9
 - 13.1 [Who can make a Request?](#) 29
 - 13.2 [What information is covered by the Act?](#) 299
 - 13.3 [What are the ICBs obligations under the Act?](#) 299
 - 13.4 [Recognising a FOI request](#) 30
 - 13.5 [Timescale for responding](#) 30
- 14.0 [Information and Data Security](#)..... 30
 - [Registration Authority/Smartcards](#) 30
 - 14.1 [Line manager responsibilities](#) 31
 - 14.2 [Staff smartcard code of practice](#) 31
 - 14.3 [Data Security](#) 31
 - 14.4 [Remote working and portable devices](#)..... 323
 - 14.5 [Remote working and portable devices best practice guidance:](#)..... 333
 - 14.6 [Portable computing devices](#)..... 333
 - 14.7 [Passwords and PIN codes](#)..... 333
- 15.0 [Network and Corporate Shared Drive Access](#)..... 344
 - 15.1 [Obtaining a Network Account](#) 344

Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

15.2 [Role Based Access](#)..... 344

15.3 [Third Party Access to Network](#)..... 355

15.4 [Prevention of Misuse](#) 355

15.5 [Software Licensing Procedure](#) 355

15.6 [Unauthorised Installation of Software](#) 366

15.7 [Individual Responsibilities](#)..... 366

15.8 [Disposal of Equipment and Reuse of Surplus Equipment](#) 366

16.0 [Internet & Intranet](#)..... 377

16.1 [Permissible Access](#)..... 377

16.2 [Non-Permissible Access](#) 377

16.3 [Monitoring](#)..... 377

16.4 [Unintentional Breaches of Security](#)..... 377

17.0 [Acceptable Use of Social Media & Social Networks](#)..... 388

17.1 [Personal use of social media at the workplace and at home](#) 388

17.2 [Using social media for professional purposes](#)..... 399

[Setting up a unique social media presence for specific service / campaign](#) 39

[Interacting with existing external social media sites](#)..... 39

[Departments considering using Social Media](#)..... 39

17.3 [Approval Process for access to Social Media](#) 40

[General usage guidance](#)..... 40

18.0 [Safe Haven Procedures - Sending Person Confidential Data or Commercially Sensitive data](#).....

[Pseudonymisation](#) 41

[Safe Haven Email Procedures](#)..... 41

18.1 [NHS Mail Encryption Facility](#)..... 41

18.2 [Safe Haven Post Procedures](#)..... 42

18.3 [Internal Post Procedures](#) 43

[Secure Bag**:](#)..... 43

[Standard Envelope:](#) 43

[External Post Procedures](#) 43

18.4 [Safe Haven Telephone Procedures](#)..... 433

[Safe Haven Room Requirements](#)..... 444

18.5 [Safe Haven Room Procedures](#) 444

Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

- 19.0 [Email](#) 455
 - 19.1 [Email Retention](#) 45
 - 19.2 [Dos and Don'ts of Email](#) 45
 - 19.3 [Sending emails to mailing/distribution lists](#) 47
 - 19.4 [Recalling emails](#)..... 47
 - 19.5 [Monitoring](#)..... 47
 - 19.6 [Long Term Absence](#) 48
 - 19.7 [Shared Email Access](#)..... 48
 - 19.8 [Accessing another user's inbox via the IT Service](#)..... 49
- 20.0 [Video and Teleconferencing via Microsoft Teams](#)..... 49
- 21.0 [Responsibilities](#) 50
 - 21.1 [Chair of Meeting/Session](#)..... 50
 - 21.2 [Meeting/Session Participants](#) 50
 - 21.3 [Training & Implementation](#) 51
- 22.0 [Data Security and Protection Incidents](#) 51
 - 22.1 [What is a data breach?](#)..... 51
 - 22.2 [What are the types of breaches?](#)..... 51
 - 22.3 [What is a Data Breach?](#)..... 51
 - 22.4 [Breach Reporting Process](#)..... 52
 - 22.5 [Investigation Process](#)..... 58
 - [Full Root Cause Analysis \(RCA\)](#)..... 58
 - [When is an incident reportable under UK GDPR/DPA18?](#)..... 58
 - [Grading the personal data breach](#) 58
 - [Breach Assessment Grid](#) 60
 - 22.6 [Sensitivity Factors](#)..... 61
 - 22.7 [Assessing risk to the rights and freedoms of a data subject](#)..... 61
- 23.0 [Records Management](#) 62
 - 23.1 [Identification/Naming of Records](#) 62
 - 23.2 [Naming of electronic records](#)..... 62
 - 23.3 [Naming conventions](#)..... 63
 - 23.4 [Naming of paper records](#) 64
 - 23.5 [Version Control](#) 64

Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

23.6 [Classification](#) 64

[Storage of Records](#) 65

[Electronic records storage](#) 65

[Paper records storage](#)..... 65

[Filing](#) 65

[Storage requirements](#)..... 65

[Indexing](#) 66

[Usage/Transfer of records](#) 66

[Access](#) 66

[Tracking and Tracing of paper records](#) 66

[Procedure for the secure movement of records during team relocation](#)..... 67

[Scope of the procedure](#)..... 67

[Preparing Records to Be Moved](#) 68

[Moving the records using an external company](#)..... 68

[Moving the records using staff members vehicles](#)..... 68

[Retention and Disposal of Records](#) 69

[Retention periods](#)..... 70

[Disposal](#) 70

25.0 [Business Continuity Plans](#)..... 71

26.0 [Digital recording of meetings](#)..... 71

[Retention of notes and recordings taken as aide-memoire for a minute taker](#)..... 72

27.0 [Information Risk Assessment and Management Programme](#) 72

28.0 [Managing Information Assets](#)..... 72

[Information Asset Register – U-Assure](#)..... 73

[Person Identifiable Data Flow Mapping](#) 73

29.0 [Data Protection Impact Assessment \(DPIA\)](#)..... 74

[Actions also to be considered](#)..... 75

[Step by Step Process to complete a Data Protection Impact Assessment](#) 76

[Information Sharing](#) 77

30.0 [Information Security Audits and Spot Checks](#) 77

[Useful Documents:](#) 79

[Contract, Temporary and Work Placement Staff Confidentiality and Compliance agreement](#) 79

Document Owner: MLCSU IG TEAM	Approval date: September 2022	First published: 18/10/22
	Next review date: September 2024	Version: 1

Consultation and Ratification Schedule

Document Name	Information Governance Handbook
Policy Number/Version:	1.0
Name of originator/author:	Midlands & Lancashire CSU Information Governance Team
Ratified by:	Integrated Care Board
Name of responsible committee:	Audit Committee
Date issued:	September 2022
Review date:	September 2024
Date of first issue:	September 2022
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of the ICB
Purpose:	To outline the standards and expectation of staffs' compliance and expected code of conduct of all staff working for the ICB
Action required:	All staff are required to read the Staff Code of Conduct declaration. 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. The code of conduct is completed via an electronic form.
Cross Reference:	Information Governance Staff Code of Conduct/ 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 intranet / internet 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 intranet / internet.

Version	Date	Author	Changes
---------	------	--------	---------

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

1.0	Sep 2022	MLCSU IG Team	First release of document for ICB
-----	----------	---------------	-----------------------------------

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	ICB	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	CoC	A set of rules to guide behaviours and decisions in a specified situation

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Term	Acronym	Definition
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.
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 Processing Agreement	DPA	<p>The Data Controller has a legal responsibility to ensure that anyone they ask to process personal information on their behalf understands what their role is and what processing they can do.</p> <p>The controller is responsible for assessing that its processor is competent to process personal data in line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects. This is because Article 28(1) says a controller must only use a processor that can provide "sufficient guarantees" (in particular in terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals.</p>
Data Processor	DP	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Term	Acronym	Definition
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	DSP Toolkit	The DSP Toolkit is the standard for cyber and data security for healthcare organisations. Organisations measure performance against the National Data Guardian's 10 data security standards.
Data Sharing Agreement	DSA	An Agreement outlining the information that parties 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
UK General Data Protection Regulation	UK 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 and on the free movement of such data (General Data Protection Regulation) 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.
Information Assets	IA	Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Term	Acronym	Definition
Information Asset Assistants	IAA	Information Asset Assistants ensure that policies and procedures are followed within their area. Recognise actual or potential security incidents. Consult your IAO on incident management Ensure that information assets registers are accurate and up to date.
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'.
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 ICS area
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.
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	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

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Term	Acronym	Definition
		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 lifecycle 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	<p>Board member with overall responsibility for:</p> <p>The Information Governance & Data Security and Protection Policies</p> <p>Providing independent senior board-level accountability and assurance that information risks are addressed</p> <p>Ensuring that information risks are treated as a priority for business outcomes</p> <p>Playing a vital role in getting the institution to recognise the value of its information, enabling its optimal effective use.</p>
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.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Information Governance – Top Do's and Do Not's

Please ensure that you follow information governance guidelines regardless of working location.

You need to bear in mind the following points -

- Who can see your screen? (Are you sitting with your back to a window where someone who looked through the window would be able to see information is on your screen)
- Lock your screen (please remember regardless of where you are, if you are going to leave your computer even if it is only to make a drink, please ensure that you lock your screen)
- Who can hear your telephone conversations? (When speaking to people on the telephone or via teams please remember there may be people in the room with you who should not have access to the information they may be hearing and therefore ensure that all private conversations are carried out ensuring that confidentiality is a priority at all times)

General Do's and Do not's

Do's

- Do familiarise yourself with information governance policies and the contents of this Handbook
- Do seek advice/guidance if you are unsure at any time with regards confidentiality, privacy, or security of personal information
- Do report anything suspicious regardless of your working location
- Do safeguard the confidentiality of all person identifiable or confidential information
- Do clear your work area of confidential information at the end of each day
- Do lock your computer screen if you leave your work area for any length of time regardless of your working location (Ctrl, Alt, Delete and Enter or Windows Key and L)
- Do ensure that you cannot be overheard when discussing confidential matters
- Do share only the minimum information necessary
- Do transfer person identifiable or confidential information securely, when necessary, i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gov.uk or use the encryption facility on nhs.net
- Do use email 'cc' or 'bcc' with care
- Do report any actual or suspected breaches of confidentiality or loss of information/data. Use your organisation's incident reporting process or via your line manager
- Do maintain your annual information governance training and read, sign the electronic code of conduct form
- Do ensure confidential information is disposed of correctly

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Do Not

- Do not share login or passwords or leave them lying around for others to see
- Do not share person identifiable information unless there are statutory grounds to do so
- Do not use person identifiable information unless necessary
- Do not collect, hold, or process more information than you need, and do not keep it for longer than necessary
- Do not discuss sensitive information in public
- Do not download from doubtful sources
- Do not use illegal software
- Do not leave sensitive information unattended
- Do not plug in USB such as Data/Memory Sticks or other devices without permission from IT
- Do not open suspicious emails
- Do not open attachments in an email if you are unsure where they have been sent from. Forward the email to your IT helpdesk and ask them to open it
- Do not have white boards etc. with personal / corporate information in view by public

Information Governance Handbook

1.0 Introduction

This handbook is intended to provide information to support and assist staff in meeting their obligations regarding good Information Governance and should be read in conjunction with the Information Governance Code of Conduct and Information Governance & Data Security and Protection Policies.

Information Governance (IG) is the practice used by all organisations to ensure that information/data is efficiently managed and that appropriate policies, system processes and effective management accountability provides a robust governance framework for safeguarding information.

IG enables organisations to embed policies and processes to ensure that personal and sensitive information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

NHS organisations hold large amounts of personal, personal confidential and sensitive information. All staff should be able to provide assurance that IG standards are incorporated within their working practices.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Personal and sensitive information can be contained within a variety of documents. For example:

- Health Records
- Staff Information
- Corporate Information
- Commissioning Information

Although this handbook provides overarching support to all staff working for the ICB, the ICB acknowledges that in some circumstances, there is a requirement for team specific Standard Operation Procedures (SOPs) to be developed to support the processes outlined in this handbook.

- These will include, but not be limited to:
- Team retention periods for the records processed within that team
- Procedures to ensure data quality – the identification and management of data errors
- Individual rights – to ensure that where an individual exercises one of their rights, the request can be actioned

2.0 Legislation and Regulations

All staff should be aware of the legislation surrounding Information Governance that stipulate how organisations should safeguard information, what processes are in place to use, secure and transfer information and also how patients and members of public have access to personal/business information.

Organisations must comply with the following:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003-17
- Environmental Information Regulations 2004
- Health and Social Care Act 2012
- Common Law Duty of Confidentiality
- Access to Health Records Act 1990
- Human Rights Act 1998
- Public Records Act 1958
- Computer Misuse Act 1990

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

3.0 Principles of the UK General Data Protection Regulation/Data Protection Act 2018:

- **Lawful, fair, and transparent processing** – this principle emphasises transparency for all UK 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.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- **Purpose limitation** – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place.
- **Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant, and limited.
- **Accurate and up-to-date processing** – this principle requires data controllers to make sure information remains accurate, valid, and fit for purpose.
- **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.
- **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).

UK GDPR also requires that:

- **Accountability and liability** – this principle ensures that organisations can demonstrate compliance.

4.0 Appointment of Data Protection Officer

Under UK GDPR/DPA18 the appointment of a Data Protection Officers (DPO) is mandatory for NHS organisations. It is especially important for health organisations which will be processing personal and sensitive information daily.

(More details about the UK GDPR/DPA18 principles can be found in the Information Governance Policy)

5.0 Caldicott Guardian Principles

All NHS employees must be aware of the eight Caldicott Principles which apply to both patient and staff data.

Previous Caldicott reviews have made recommendations aimed at improving the way the NHS uses and protects confidential information.

Principle 1: Justify the purpose for using confidential information - Why is the information needed?

Principle 2: Use personal information only when it is necessary – Can the task be carried out without identifiable information?

Principle 3: Use the minimum necessary personal information – Can the task be carried out with less information?

Principle 4: Access to confidential information should be on a strict need-to-know basis – Only those who need access, should have access.

Principle 5: Everyone with access to personal identifiable information should be aware of their responsibilities – Lack of knowledge is not acceptable

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Principle 6: Comply with the law – Every use of confidential information must be lawful

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

Principle 8: Inform the patients and service users about how their confidential information is to be used – Patients and service users should be given an accessible way to opt out

6.0 Confidentiality

Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff, or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality.

This handbook sets out the key principles and main ‘dos and don’ts that everyone should follow to achieve this for both electronic and paper records.

The common law of duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

Personal Confidential Data is information about any living individual who can be identified from that data.

Such person-identifiable information may be manually held or automated and includes for example, the contents of filing cabinets, all patient information, including medical records, photographs, x-rays, and other images, computer disks, tapes, CD ROMs etc.

Personnel records include those held by line managers, as well as those held centrally by personnel departments.

The use of all such personal data is controlled by the UK GDPR/DPA18 principles above.

7.0 Summary of key roles and responsibilities

Senior Information Risk Owner

The Senior Information Risk Owner is an executive Board member with allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at Board level. Cheshire and Merseyside ICB have nominated Prof. Rowan Pritchard-Jones, Medical Director as the SIRO.

Information Asset Owners

The SIRO is supported by Information Asset Owners (IAOs) whose role is to understand what information is held, what is added and what is removed, who has access and why in their own area.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Information Asset Assistants

Information Asset Assistants support the IAOs in ensuring that policies and procedures are followed in their areas. Alerting the IAO to actual or potential security incidents. Ensuring that the information assets register, and data mapping tool is accurate and up to date.

Caldicott Guardian

The Caldicott Guardian is the person with overall responsibility for protecting the confidentiality of personal confidential data (PCD) and for ensuring it is shared appropriately and in a secure manner. Cheshire and Merseyside ICB have nominated Christine Douglas, Director of Nursing and Care, as the Caldicott Guardian.

Data Protection Officer

The Data Protection Officer is a role mandated by UK GDPR and is involved in all issues which relate to the protection of personal data. Cheshire and Merseyside ICB have nominated Hayley Gidman, Head of Information Governance at Midlands and Lancashire Commissioning Support Unit, as the Data Protection Officer.

Information Governance Team

The Information Governance Team is responsible for ensuring that the Information Governance program is implemented throughout the organisation.

Please contact the **IG Service Hub** on **Tel: (01782) 872648** or **Email: mlcsu.ig@nhs.net**

The Information Governance Team is also responsible for:

- The completion and annual submission of the Data Security and Protection Toolkit requirements
- Support in investigating Serious Incidents Requiring Investigation (SIRIs)
- Offering advice and ensure the organisation complies with legislation, policies, and protocols.
- Providing specialist IG training. All training sessions are conducted remotely and to see what training is available and to book a place please click onto the link [specialist IG training](#)

8.0 Secure Working Environment - Premises security & Off-Site Working

8.1 ID Badges

All staff should wear their ID badge whilst on the organisations premises or when representing the organisation. ID badges are personal to the user and should not be passed to unauthorised personnel or loaned to other members of staff.

Managers should ensure that any member of staff, whether permanent or temporary, hand in their ID badge on their last day of employment.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

The loss of an ID badge should be reported immediately to your line manager and an incident logged, although please note that this would not be an IG breach as it is not a breach of data protection or confidentiality.

8.2 Access Control

It is essential that access is tightly controlled throughout the organisation's premises. Where possible all access to work areas should be restricted.

Visitors should be asked to report to a reception where they will be asked to sign the visitors book recording their name, business, the person they are visiting, time of arrival and departure and then be met by the person who has invited them. Where at all possible, visitors should make appointments in advance and "cold calling" should be strongly discouraged. At the end of the meeting, the visitor will be escorted back to the reception area to sign out prior to departure.

Members of staff who require access through any door which is controlled via digital door locks or proximity access systems, will be issued with the appropriate code numbers or personal fobs/cards to ensure the security of the area is maintained at the highest level. Code numbers must be kept secure and must never be given to visitors. Such doors should never be latched or wedged open.

Staff should not release any door with controlled access without first checking the identity of the person seeking entry.

Where entry to a working area is by coded access, these codes must be changed on a regular basis or whenever it is felt that the code may have become compromised.

Staff should also be aware of other persons "tailgating", i.e. attempting to gain access to a controlled access area by closely following them as they enter. If the person is not recognised as a member of staff, or authorised visitor, he/she should be asked to:

- Wait at the door or in a designated waiting area
- Give details of the person, with whom they have an appointment
- Await the arrival of an identified member of staff to escort them into the controlled access area
- At the end of the appointment / meeting the visitor should be escorted out of the controlled access area

Staff are expected to challenge anyone found in non-public areas not displaying a name badge, firstly to ensure that they have a legitimate reason for being there and secondly to remind them of the organisation's expectations with regard to use of identity badges.

When working off-site either at home or another location staff must consider confidentiality when holding conversations or using a screen. Aspects to consider:

- A working space shared with family members, friends, or members of the public, conversations should be held where they are less likely to be overheard and screens positions where they are less likely to be overseen

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Do not leave devices unattended or logged on
- To avoid loss or theft of confidential data, store paper and devices in a secure area at the end of the working day not accessible to other members of the household

8.3 Printing From Home

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

8.5 Clear Screen & Clear Work Area

Clear Screen

- Laptops, PCs and mobile devices should be locked when they are not in use regardless of working location (i.e. working in a solitary location) and how long they will be left unattended (i.e. to go to the toilet, make a cup of tea or to speak to a colleague at their desk, etc.). For Windows based systems, this can be completed by pressing **Ctrl – Alt – Delete** and then **ENTER** or holding the Windows Key and pressing **L**.
- On the occasions when there is a genuine mistake and screens are not locked, the password protected screensaver will launch after 7 minutes idle

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

time. This should however only be used as a 'back up' for when the screen is not locked.

- You should always shut down your PC/laptop when finishing work for the day. This enables any security and system updates to be rolled out and installed when the device is restarted. When working remotely please follow the IT security Guidance to ensure mobile devices remain secure.
- Computer and laptop screens should always be angled away from the view of unauthorised persons, being mindful of where they are positioned in relation to walkways and windows. Additional care should be considered whilst working remotely always be aware of who may see the screen. (i.e. sitting with back to a window, is the room being used by others, family, friends, the public?)

Clear Work Area

- Where practically possible all confidential papers and removable media, including laptops etc. should be stored in suitable locked cabinets or other forms of security furniture when they are not in use, especially outside of working hours regardless of where you are working.
- Staffs who are required to attend meetings or leave their work area unoccupied for any amount of time should remove any confidential information from their work area.
- Where lockable filing cabinets, drawers, cupboards etc. are not available, office/room doors must be locked if left unattended. At the end of each day all sensitive information should be removed from the workplace and stored in a locked area. This includes all person identifiable information, as well as business confidential information such as salaries and contracts.
- Staff should also be aware that information left on their work area is more likely to be damaged or destroyed in a disaster such as fire, flood, Spillages etc.
- Any visitor, appointment or message books should be stored in a locked area when they are not in use.
- Staff working remotely should ensure their 'working area' is cleared at the end of the day ensuring papers and working devices are securely stored regardless of where you are working.

9.0 Information Governance Induction for New Starters

It is vitally important that all new staff are made aware of the ICB Information Governance requirements at the earliest opportunity and clear guidance is given about their own individual responsibilities for compliance. Emphasis must be placed on how IG requirements affect their day to day work practices. It is equally imperative that IG remains embedded with each individual throughout their daily working practices.

To facilitate this, the IG team will provide an IG induction to all new starters remotely. To book onto a training session please click on the following link.

<https://bookwhen.com/csu>

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

10.0 Annual Information Governance Training

All staff are mandated to complete annual IG training. The training is available as an e-learning module accessed via the ESR System.

If you or your line manager feels that you require further specialist IG training, e.g. for information risk, IAO or IAA responsibilities or completing Data Protection Impact Assessments (DPIA), please click onto the link to book onto a remote training session. [specialist IG training](#)

11.0 Individual's Rights

Individuals legally have rights in relation to the data that is processed about them. The ICB must have processes in place should an individual choose to exercise any of their rights. It is vital that all staff can recognise such requests to allow them to be processed within the timescales set out in law.

11.1 The right to be informed

The ICB has a privacy notice which is available primarily through its public facing website at <https://www.cheshireandmerseyside.nhs.uk/>. The purpose of the privacy notice is to inform the public about the collection and use of their personal data. All ICB staff need to be aware of this notice and be able to direct individuals both to the notice and to where they can contact if they have any queries or concerns, usually the Data Protection Officer.

In addition to the privacy notice, the ICB will also provide individuals with more specific information at the time personal data is collected from them, for example when an application of Continuing Healthcare is made, a complaint is made, or an individual signs up to be part of an engagement group. As it will vary as to when further information will need to be provided to individuals, the CSU IG team should always be consulted to determine what is required in each circumstance

Alongside this, the ICB also has an internal privacy notice which explains to ICB employees how the ICB processes their data.

11.2 The right of access

Individuals, including staff, have the right to ask the ICB for confirmation of whether they process data about them, and if the ICB does, to have access to that data so the individual is aware and can verify the lawfulness of the processing.

This is called a Subject Access Request and the process around this is detailed further on in this handbook.

11.3 The right to rectification

If personal data that the ICB holds is found to be inaccurate or incomplete, individuals have the right to have it rectified. This includes any data that the ICB may have passed on to others unless this proves impossible or involves disproportionate effort. If this is the case, the ICB will explain to the individual why this has not been possible.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

The individual can make a request for rectification either verbally or in writing and the ICB has one calendar month to respond to such requests.

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICBs Data Protection Officer is made aware of the request, make sure that the request is recorded and support the ICB to acknowledge and then consider the request. If it is determined that rectification is required, the ICB must ensure that any recipients of the data that is to be rectified are informed that the data has been shared with them **Hayley Gidman, Data Protection Officer mlcsu.dpo@nhs.net**

The right to rectification is not an absolute right. Requests deemed to be unfounded, excessive, or repetitive in nature can be refused. Additionally, If the records in question need to be maintained for the purposes of evidence (such as information relating to a potential safeguarding concern) requests may also be refused

The ICB does not have overarching processes for rectification of data as this will vary in each circumstance such a request is made and depending on how the data to be rectified is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

11.4 The right to erasure

The right to erasure is also known as 'the right to be forgotten' and means that individuals have the right to have personal data that the ICB hold about them erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If the individual withdraws their consent for the ICB to process their data (if this was the basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data must be erased in order to comply with a legal obligation.

However, if the ICB have collected and are processing data about you to comply with a legal obligation for the performance of a public interest task or exercise of official authority, i.e. because the ICB has a legal duty to do so in their functioning as an ICB, or because the processing is necessary for the provision of health or social care/ for the management of health or social care systems or services, then the right to erasure does not apply.

Requests for erasure can be made both verbally or in writing and the ICB has one calendar month to respond to such requests.

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICB Data Protection Officer is made aware of the request, make sure that the request is recorded and support the

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

ICB to acknowledge and then consider the request. If it is determined that data should be erased is required, as in some circumstances such a request can be refused, the ICB must ensure that any recipients of the data that is to be erased are informed that the data has been shared with them will also need to be erased.

The ICB does not have specific processes for erasure of data as this will vary in each circumstance such a request is made and depending on how the data to be erased is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

11.5 The right to restrict processing

This right means that individuals have the right to ‘block’ or suppress processing of their personal data which means that if they exercise this right, the ICB can still store their data but not to further process it and will retain just enough information about the individual to ensure that the restriction is respected in future.

Individuals can ask us the ICB to restrict the processing of their personal data in the following circumstances:

- If they contest the accuracy of the data the ICB hold about them, the ICB will restrict the processing until the accuracy of the data has been verified.
- If the ICB are processing the individual’s data as it is necessary for the performance of a public interest task and the individual has objected to the processing, the ICB will restrict processing while they consider whether their legitimate grounds for processing are overriding.
- If the processing of the individual’s personal data is found to be unlawful but they oppose erasure and request restriction instead; or
- If the ICB no longer need the data held about the individual, but the individual requires the data to establish, exercise or defend a legal claim.

There are a number of different methods that could be used to restrict data, such as:

- temporarily moving the data to another processing system
- making the data unavailable to users; or
- temporarily removing published data from a website

Requests for restriction can be made both verbally or in writing and the ICB has one calendar month to respond to such requests.

As there are close links between this right and the right to rectification and the right to object, as a matter of good practice, the ICB should automatically restrict processing whilst requests to exercise those rights are considered.

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICB Data Protection Officer is made aware of the request, make sure that the request is recorded and support the ICB to acknowledge and then consider the request.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

If the ICB have disclosed the personal data in question to others, the ICB will contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, the ICB will also inform the individual about these recipients.

The ICB will inform the individual if it decides to lift a restriction on processing.

The ICB does not have specific processes for restriction of data as this will vary in each circumstance such a request is made and depending on how the data to be restricted is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

11.7 The right to data portability

The right to data portability allows the individual to obtain and reuse personal data they have provided to the ICB for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

It does however only apply where the ICB are processing the personal data based on the individual's consent to do so, for the performance of a contract or where the processing is carried out by automated means. This means that currently, the ICB holds very limited data which would be subject to the right to data portability.

Requests for data portability can be made both verbally or in writing and the ICB has one calendar month to respond to such requests.

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICB Data Protection Officer is made aware of the request, make sure that the request is recorded and support the ICB to acknowledge and then consider the request.

The ICB does not have specific processes for data portability as this will vary in each circumstance such a request is made and depending on how the data is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

11.8 The right to object

Where the ICB necessarily processes personal data for the performance of a task in the public interest/exercise of official authority, the individual has a right to object to the processing. They must have an objection on grounds relating to their particular situation.

If an individual raises an objection, the ICB will no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override the individual's interests, rights and freedoms or the processing is for the establishment, exercise or defence of legal claims.

Objections can be made both verbally or in writing and the ICB has one calendar month to respond to such requests.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICBs Data Protection Officer is made aware of the request, make sure that the request is recorded and support the ICB to acknowledge and then consider the request.

The ICB does not have specific processes for objections to processing as this will vary in each circumstance such a request is made and depending on how the data is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

11.9 Rights in relation to automated decision making and profiling

Automated individual decision-making is a decision made by automated means without any human involvement.

Examples of this include:

- an online decision to award a loan; and
- a recruitment aptitude test which uses pre-programmed algorithms and criteria.

Automated individual decision-making does not have to involve profiling, although it often will do.

Profiling is:

“Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviours, location or movements.” [UK GDPR Article 4(4)]

As the ICB does not make any decisions based solely on automated processing, individuals’ rights in relation to personal data processed in this way are not applicable.

11.10 The right to withdraw consent

Although not specified as an individual right in UK GDPR, individuals do have the right to withdraw their consent for their data to be processed for any specified purpose. They can withdraw their consent at any time.

Where possible, the ICB will make sure that the individual is able to withdraw their consent using the same method as when they gave it.

If an individual withdraws their consent, the ICB must stop the processing of their data as soon as possible.

Should such a request be received, the CSU IG team should be contacted in the first instance. The CSU IG team will then ensure that the ICB Data Protection Officer is made aware of the request, make sure that the request is recorded and support the ICB to acknowledge and then consider the request.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

The ICB does not have specific processes for requests to withdraw consent as this will vary in each circumstance such a request is made and depending on how the data is held. Therefore, each request will be considered and acted upon on a case by case basis, with procedures in place within the team holding data to which this right may apply.

12.0 Subject Access Requests

12.1 Access to Information (Subject Access Requests -SAR)

Every living person (or their authorised representative) has the right to access personal information/records held about them by an organisation. This type of request is known as a Subject Access Request – SAR.

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.

To note – Anything documented on a corporate means of communication (work email and skype accounts, messages, e.g. WhatsApp on a work mobile) is subject to access to information legislation, i.e. SAR and FOI. If it is within scope of any request, it will be considered for release.

All Subject Access Requests can be verbal or in writing. Within all applications for access to records the applicant will need to prove their identity.

Timescales to respond to a SAR

Under UK GDPR/DPA18 information requested must be provided without delay and at the latest within **one month** of receipt, all requests for access to records should be forwarded to the SAR Team **immediately** - see below.

Fees

Under UK GDPR/DPA18 all information is to be supplied free of charge (although “reasonable” fees can be charged for an excessive request or for further copies).

Failures to meet requests for information

Failure to comply and provide information requested under UK GDPR/DPA18 could result in an enforcement action which can include a monetary penalty.

The maximum fine that can be issued by the Information Commissioner 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.

12.2 Recognising a SAR

A SAR can be made in writing or verbally; however, the requestor does not need to mention the UK GDPR 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 policy.

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

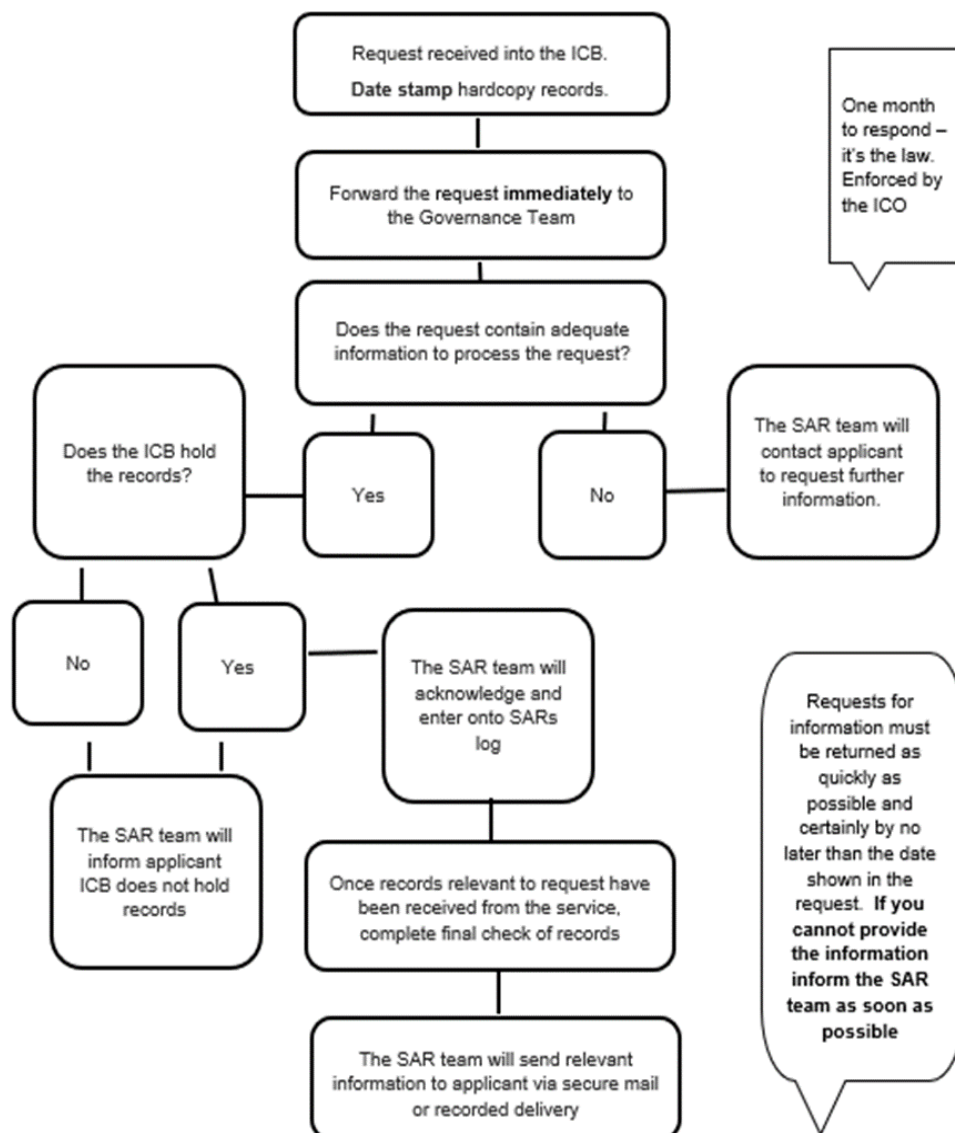
Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Email
- Verbal
- Fax
- Post
- Social media
- ICB website

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

SAR@cheshireandmerseyside.nhs.uk

12.3 SAR Flowchart



Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

13.0 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 (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

13.1 Who can make a Request?

- Anyone can make a Freedom of Information request – they do not have to be UK citizens or resident in the UK.
- Freedom of Information requests can also be made by organisations, for example a newspaper, a campaign group or a company.
- Employees of a public authority can make requests to their own employer, although good internal communications and staff relations will normally avoid the need for this.

13.2 What information is covered by the Act?

- The Act covers all recorded information held by a public authority. It is not limited to official documents and it covers, for example, drafts, emails, notes, recordings of telephone conversations and CCTV recordings. Nor is it limited to information you create, so it also covers, for example, letters you receive from members of the public, although there may be a good reason not to release them.
- Requests are sometimes made for less obvious sources of recorded information, such as the author and date of drafting, found in the properties of a document (sometimes called meta-data). This information is recorded so is covered by the Act and you must consider it for release in the normal way.
- If a member of the public asks for information, you only must provide information you already have in recorded form. You do not have to create new information or find the answer to a question from staff who may happen to know it (i.e. it is in their head)
- The Act covers information that is held on behalf of a public authority even if it is not held on the authority's premises. For example, you may keep certain records in off-site storage, or you may send out certain types of work to be processed by a contractor.
- Where you subcontract public services to a private company, that company may then hold information on your behalf, depending on the type of information and your contract with them. Some of the information held by the external company may be covered by the Act if you receive a freedom of information request.

13.3 What are the ICBs obligations under the Act?

As an organisation, there are two main obligations under the Act. The ICB must:

- publish certain information proactively.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- respond to requests for information where the information is not proactively published.

Making information available is only valuable to the public if they know they can access it, and what is available. The ICB should:

- publicise their commitment to proactive publication and the details of what is available
- publicise the fact that people can make freedom of information requests to the ICB
- provide contact details for making a request, including a named contact and phone number for any enquiries about the Act
- the ICB should communicate with the public in a range of ways. This is likely to include websites, noticeboards, leaflets, or posters in places where people access ICB services

13.4 Recognising a FOI request

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

foi@cheshireandmerseyside.nhs.uk

Timescale for responding

The deadline for a public authority to respond to requests made under the Act is **20 working days**.

The clock starts the next working day after receipt of the request it is therefore vital that all requests are forwarded to the FOI team immediately:

foi@cheshireandmerseyside.nhs.uk

If you are unsure about a request for information, contact the FOI team in the first instance.

14.0 Information and Data Security

The contents below are issued for guidance to help staff carry out their roles in a secure and safe way when dealing with personal information.

Registration Authority/Smartcards

Smartcards are required to use and access IT systems essential to healthcare provision.

Primary Care Contractors need to use Smartcards in order to gain access to patient information i.e. those who provide the Choose and Book service and the Electronic Prescription Service.

Individuals are granted access to a Smartcard by the organisation's Registration Authority lead. It is up to the Registration Authority Team to verify the identity of all healthcare staff who need to have access to patient identifiable or sensitive data.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Individuals are granted access based on their work and their level of involvement in patient care.

The use of Smartcards leaves an audit trail.

Staff should be aware that disciplinary action may be taken if Smartcards are shared or lost.

14.1 Line manager responsibilities

- To identify all roles within their area of responsibility which require access to the system and ensure that all employees, including temporary/agency/bank and locum employees, are provided with appropriate access.
- To ensure for all roles that involve access to the system that job descriptions and any recruitment materials make reference to the need to be registered and the role's responsibilities in relation to using the system.
- To ensure that all new starters within their area of responsibility, including agency/temporary employees, receive training in order to be able to access the system.
- To ensure that all employees are aware of Information Governance policies, associated documentation and their responsibilities in relation to use of and access to the system.
- To immediately inform the Registration Authority Team, of any leavers, starters and staff changes.

14.2 Staff smartcard code of practice

- Use your Smartcard responsibly and in line with your access rights.
- Inform the Registration Authority team or the IG team immediately should your Smartcard be lost, stolen or misplaced.
- Ensure that you report any misuse of the Smartcards
- Ensure that you keep your Smartcard and log-in details confidential. You must not leave your PC logged in and you must not share or provide access to your Smartcards or passwords.
- Ensure that you accurately complete the necessary paperwork, provides suitable identification, and attends any appropriate appointments in order to register on the system or have your Smartcard updated/re-issued.
- All members of staff using Smartcards should follow the organisation's suite of Information Governance policies and procedures; adhere to the UK GDPR and Caldicott Principles, and the Confidentiality Code of Practice and the Care Records Guarantee.

TO RAISE ANY SMARTCARD ISSUES PLEASE CONTACT THE IT SERVICEDESK FOR YOUR PLACE BASE.

14.3 Data Security

Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Information, whether in paper or electronic form, is of high importance to the ICB, therefore the organisation must ensure that the information is properly protected and is reliably available.

- Access to all confidential or sensitive information whether held on paper or electronically must be restricted.
- Staff must ensure that doors and windows are closed properly, blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team or it is suspected that someone else knows the code.
- All employees should wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access (see premises security above). Visitors should be met at reception points and accompanied to appropriate member of staff or meeting and should be asked to sign in and out of the building.
- Employees on termination of employment or contract must surrender door keys, Smartcards, and all relevant equipment in compliance with the ICB leavers' process.
- All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset.
- All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. The organisation will investigate all suspected and actual security breaches.

14.4 Remote working and portable devices

The developments with information technology have enabled staff to adapt to more flexible and effective working practices, by providing mobile computing, video conferencing via Teams and portable devices.

When using video conferencing i.e. Teams please make sure that you are aware of who is on the call/ meeting.

Extra care and precaution should be exercised whilst sharing your screens or conducting a training session. It is best practice to close all screens that you do not need for the meeting/ training session to ensure that the incorrect screen is not shared.

Although these working practices are advantageous, it is important for all staff to understand the associated risks to the information, and the responsibility to ensure that information accessed remotely or held on portable devices, is protected by adequate security.

It is important for staff to protect information which is processed remotely or is stored on portable devices and staff should read relevant policies to ensure good practice.

Staff are responsible for the security of any portable devices issued to them, and should take all necessary precautions to avoid loss, theft, or damage. In the event of loss, damage or theft occurring, they must report this immediately to their line manager and ICT service desk.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Remote working and portable devices best practice guidance:

- Encryption is mandatory in all mobile devices used to store identifiable data.
- Any portable computing device must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, ensure that it is safely stored out of sight.
- Staff should take extra vigilance if using any portable computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the organisation's stored information by a third party "overlooking". There are security measures which can be deployed to support this if such travel is common to the role, staff should enquire through their line managers.
- Staff should not leave the device unattended for any reason unless the session is "locked" and it is in a safe working place, devices should not be left in an unattended publicly accessible room for example. If possible, staff should take the device with them.
- Ensure that other 'non' authorised users are not given access to the device or the data it contains.
- When using a portable device check the internet access is secure (e.g. use a Virtual Private Network and/or if possible, avoid public wi-fi) and that any security features are in use.
- When working from home or other alternate locations it may become your responsibility to maintain the monthly Microsoft Patch updates on laptops as this may not be possible to roll out centrally. Follow guidance supplied by the ICB IT service if required.

Portable computing devices

- Sensitive corporate and PCD must not be stored or transferred using any unencrypted "USB Memory" device.
- Where it is not possible to encrypt sensitive/personal information, the advice of the IG team should be sought and, a one-off data transfer solution should be found using a secure method.
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available.
- Information should not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible.
- Staff must ensure that any suspected or actual breaches of security are reported to their line manager.
- Staff must ensure that the mobile devices are always used appropriately.
- Staff should not under any circumstances use any mobile device whilst in control of a vehicle.
- All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information.

Passwords and PIN codes

Passwords should be a combination of letters and digits of a pre-determined length and combination of characters, typically using the lower case of the keyboard.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Passwords and/or PINs should not normally be written down, but if unavoidable, should be held on your secure drive in a passwords folder and never kept with the device or in an easily recognisable form. Passwords MUST be minimum length of 10 characters without requiring a mix of character types.

- Not matching your previous four passwords.
- Not detected as a common password, e.g. password1234; and
- Not detected as a breached password (a password used for an account that has previously been compromised).
- No complex security requirements.

Where the above standard is not appropriate or supported by the application or system and the ICB has approved the use of the system, password should be created in the following format:

- A minimum of 8 characters long
- Contain at least one uppercase letter
- Contain at least one lower case letter

and one of the following options

- Contain at least one number
- Contain at least one special characters or non-alphanumeric characters, such as:
 - ! " £ \$ % & * @.

15.0 Network and Corporate Shared Drive Access

15.1 Obtaining a Network Account

It is NHS policy that all staff should have access to email. To use email, you require a network account. You also require an account to access the shared network drives.

Managers should contact the IT service to request a New User access form which they should then complete and return to the IT service to allow a new network account to be created.

It is the responsibility of line managers to notify the IT Service of changes in staff circumstances that may affect access to systems. These include job title, work location, maternity/sick leave. Managers should also notify the IT Service Desk of all leavers so that their network account can be disabled.

It is the user's responsibility to chase the IT Service to ensure that their network account is created in a timely manner. Please note that under no circumstances should another person's account be used in the interim if your account has not yet been set up.

15.2 Role Based Access

- Users will only be granted access to data and information that it is required as part of their job. Access is therefore granted on a 'need to know' basis.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Access authorisation should be regularly reviewed, particularly when staff roles and responsibilities change. This is the responsibility of line managers.
- Staff must not access computer systems or data unless they have authority to do so. Access to files which are not in the course of the employee's duty will be considered a disciplinary offence. For example, accessing a friend or relative's manual or electronic file. This may also be deemed a breach of the Computer Misuse Act 1990 and UK GDPR/DPA18.
- Access should be requested via your line manager.

15.3 Third Party Access to Network

Third parties will not be given access to the organisations systems or networks unless they have formal authorisation to do so. All non-NHS companies will be required to sign security and confidentiality agreements with the organisation.

Where the third party has access to NHS patients and/or to their information; is providing support services directly to an NHS organisation; and/or has access to national systems and services, including N3, Choose and Book etc. they are required to provide IG assurances via the DSP Toolkit as part of business/service support processes or contractual terms. That is, for these organisations annual DSP Toolkit assessments are required for either or both of two purposes:

- a) To provide IG assurances to the Department of Health or to NHS commissioners of services.
- b) To provide IG assurances to NHS Digital as part of the terms and conditions of using national systems and services including HSCN, Choose and Book etc.

Third parties found accessing elements of the system to which they are not authorised will be deemed to have caused a data breach and will be denied access to the network immediately. An incident will be recorded following the organisations incident reporting process and an investigation will take place to decide the outcome.

15.4 Prevention of Misuse

Any use of IT facilities for non-business or unauthorised uses without management approval will be regarded as inappropriate usage.

The Computer Misuse Act 1990 introduced three criminal offences. Staff must remember that the following offences can be enforced in a court of law:

- Unauthorised access
- Unauthorised access with intent to commit further serious offence
- Unauthorised modification of computer material

15.5 Software Licensing Procedure

New software, which has not been properly developed and/or properly tested, is a threat to the security of existing data and systems. All software and hardware procurements shall take account of the security requirements recommended by the IG team. Contravention of the recommendations may be considered a disciplinary offence.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

15.6 Unauthorised Installation of Software

Unauthorised software poses a risk to your computer, other computers and the network as a whole from malicious code embedded within the software. The risk applies to all programs and games downloaded from the Internet, CD/DVD or any other storage media. Malicious code may be computer viruses and spyware, and the effects will vary depending on which has been downloaded.

A second and equally important reason why you should never use unauthorised software is because of licensing issues. The organisation is required to purchase licenses for the use of all software on its systems. If you install software without authorisation this process is by-passed, and you put the organisation at risk of legal action from the owner of the software. If you are installing so-called free software, it could be an illegal copy, or it could be trial software with an expiry date. Even if neither of these things apply, the software is likely to be for single personal use and require a license for corporate use.

It is a breach of security to download files which disable the network, or which have the purpose of compromising the integrity and security of the organisation's networks and/or file servers. To intentionally introduce files which cause damage to computers may result in prosecution under the Computer Misuse Act 1990.

15.7 Individual Responsibilities

Individuals must not install software onto an organisation provided desktop, laptop or another mobile device. Doing so constitutes a disciplinary offence. A request for installation should be made to the IT Service.

The IT Service audits all computer equipment including software. If unauthorised software is found on a system or if no license agreement has been purchased, IT Service staff are authorised to remove the software.

Should you suspect the presence of unauthorised software on your system you should report it to the IT Service, who can also advise on the procedure for purchasing software licenses.

It shall also be considered a disciplinary offence to connect any new hardware/equipment to the network without prior approval from your line manager and the IT Service.

15.8 Disposal of Equipment and Reuse of Surplus Equipment

Departments should follow a general policy of internal cascading of any surplus equipment within their own area.

Should it not be possible to reuse equipment internally within the organisation, once all information has been removed from any hardware and backed up where necessary, users must request that all hard disks within the hardware are destroyed by the IT service.

This is to ensure that the organisation:

- Complies with obligations under European Environmental Legislation.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Fulfils its commitment to the Waste Reduction Policy 1996 and Sustainability Policy 2000.
- Meets software license obligations and reduces the risk of sensitive data being made available to unauthorised persons.

16.0 Internet & Intranet

16.1 Permissible Access

Access to the internet is primarily for work or for professional development and training.

Reasonable personal use is permitted during your own time (for example, during your lunch break), provided that this does not interfere with the performance of your duties. Personal access to the internet can be limited or denied by your manager. Staff must act in accordance with their manager's local guidelines. The organisation has the final decision on deciding what constitutes excessive use.

The internet must never be assumed to be secure. Confidential information or data must never be transmitted over the internet unless the data or information is encrypted. Information obtained through the internet may not be accurate, and users must check the accuracy, adequacy or completeness of any such information.

16.2 Non-Permissible Access

No member of staff is permitted to access, display or download from internet sites that hold offensive material. To do so may constitute a serious breach of the organisations security and could result in disciplinary action, dismissal and/or criminal prosecution. Offensive material includes hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. Users must not create, store or distribute any material that is libellous, blasphemous or defamatory. This list is not exhaustive. Other than instances which demand criminal prosecution, the organisation is the final arbiter on what is or is not offensive material, or what is or is not permissible access to the Internet.

If a web page cannot be accessed, it is possible that the site has been banned and access to the website has been blocked. Sites that are added to this list include ones which contain offensive content i.e. pornographic, terrorist, racist etc. If you require access to a blocked site permission must be gained from your line manager and IT.

16.3 Monitoring

You should be aware that a range of monitoring is conducted on internet usage. This indicates time spent on the internet and list of visited websites. Logs of internet usage are used to investigate allegations of misuse.

16.4 Unintentional Breaches of Security

If you unintentionally find yourself connected to a site that contains offensive material, you must disconnect from the site immediately and inform your line manager and the IT Service Desk.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

17.0 Acceptable Use of Social Media & Social Networks

NHS organisations of all types are now making increased use of social media and social networks to engage with their patients, other stakeholders, and to deliver key messages for good healthcare and patient services generally. These online digital interactions are encouraged, and their use is likely to be further extended as new communications channels become available. Social media has great potential to help the NHS reach patients and service users that do not engage using traditional communications and engagement channels. However, the inappropriate or ill-considered use of social media also has the potential to damage both individual's and the NHS' reputation. It is therefore important that staff are aware that there are several legal implications associated with the inappropriate use of social media. Liability can arise under the laws of defamation, copyright, discrimination, contract, human rights, protection from harassment, criminal justice act etc. This list is however non-exhaustive.

Social media describes the online tools, websites and services that people use to share content, profiles, opinions, insights, experiences, perspectives, and media itself. These tools include social networks, blogs, message boards, podcasts, microblogs, image sharing, social bookmarking, wikis, and vlogs. Internal SharePoint sites also provide social networking capabilities and are included in this procedure. The feature that all these tools, websites and services have in common is that they facilitate conversations and online interactions between groups of people.

It is important that all staff and contractors have a general awareness of the information risks and good practices associated with the protection of sensitive information in social media and other social interaction scenarios.

External social media sites must not be used to exchange any work-related information between colleagues or organisations, for example in place of using email.

The organisation has the right to manage its reputation on all levels, including any employee interaction on social networking sites that could possibly reflect an opinion upon the organisation.

17.1 Personal use of social media at the workplace and at home

This section of the procedure provides guidance on the use of social media tools by NHS employees in a personal capacity. For example, this includes a personal profile on Facebook or use of Twitter in a personal capacity by NHS employees.

It is important to remember that adherence to the expectations set out in this handbook applies equally whilst not at work when any inference is made to work, either specifically or indirectly.

All policies apply equally inside and outside of work hours when work related.

Staff or contractors must be aware of their association with the organisation when using social media. If they identify themselves as an employee of a specific NHS organisation, they should ensure that their profile and any related content is

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

consistent with how they would wish to present themselves with colleagues, patients, and service users.

Staff or contractors who may not directly identify themselves as an NHS employee when using social media for personal purposes at home, should be aware that content they post on social media websites could still be construed as relevant to their employment at the organisation. For example, employees should not write or report on conversations, meetings or matters that are meant to be private or internal to the organisation.

Unauthorised disclosure of confidential information would constitute misconduct/gross-misconduct in accordance with the organisations disciplinary policy. **Employees must not cite or reference patients, service users, partners or providers without their written approval.**

The organisation will not accept liability for any consequences arising out of employee's personal use of social networking sites.

17.2 Using social media for professional purposes

This relates to the use of social media tools by NHS employees in the course of carrying out their normal duties in delivering NHS services. For example, this would include using a Facebook page to promote NHS activities and initiatives.

Setting up a unique social media presence for specific service / campaign

This can be used to:

- Enhance engagement with a target audience. This is likely to work best for specific campaigns or issues (e.g. Quit smoking – through privileged access to content and information for 'Facebook friends'; information re: prize draw winners; uploading event photos, etc.)
- Allow service users to share experiences
- Promote specific events via invites and newsfeeds
- Drive traffic to the official website where more information is available
- Send information/support directly to service users mobiles (e.g. via Twitter)

Interacting with existing external social media sites

This can be used to:

- Engage with other service providers – creating a virtual network of relevant professionals to share and disseminate information and good practice and to act as a hub on relevant topics
- Monitor what is being said online about the organisation and its services, and give an authorised user the right-to-reply
- Drive traffic to the organisation's website and social media pages

Departments considering using Social Media

Certain considerations must be made when scoping the use of Social Media.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Moderating the site must be done on a 365-day basis, in order that any malicious or malevolent comments are removed as soon as possible. This must be undertaken within the department.
- Disclaimers on social media sites do not remove the organisation’s obligations to accuracy and implications.
- Comments made to a social network site belonging to the organisation can be disclosed under the Freedom of Information Act 2000.
- When the organisation (or department within the organisation) creates an account on a social networking site such as Twitter or Facebook, the Information Commissioner has dictated that the organisation must be in a position to receive a Freedom of Information/Environmental Information Request via that medium.
- If an FOI or EIR request is received via this medium, you must notify and forward it to the FOI team immediately.

17.3 Approval Process for access to Social Media

Any staff member wishing to set up a social media presence OR interact with existing external sites where they are identified as an organisation employee MUST follow the following procedure:

- Obtain approval from relevant Line Manager and Director
- For communications on behalf of the organisation, any other NHS services, or a partnership of which the organisation is a member, a business case should be made which will be considered and referred to directors with recommendations. The Information Governance, Human Resources and Communications team should be consulted during this process.
- For staff or contractors wishing to use an NHS or other professional website or social media tool during working hours to share best practice or seek advice and feedback from other colleagues as part of their role, they should gain the appropriate authorisation from their line manager before proceeding. Line managers unsure of which sites, forums or tools are acceptable for use should speak to the Information Governance team for advice.

General usage guidance

When using social media, employees should respect their audience. As a rule, employees should be mindful of any detrimental comments made about colleagues whilst using social media. Any conduct which breaches the employee code of conduct such as failing to show dignity at work (harassment), discriminatory language, personal insults, obscenity, and disclosure of confidential information will be considered a disciplinary matter. These examples are not exhaustive.

Staff and contractors should also show proper consideration for others’ privacy and for topics that may be considered sensitive or controversial.

Staff and contractors are encouraged not to divulge who their employers are within their personal profile page (e.g. in accordance with RCN guidelines, “RCN Legal Advice on using the internet”). However, those that do divulge their employer should state that they are tweeting/blogging etc. in a personal capacity.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Staff and contractors must not share details of the organisation’s implemented security or risk management arrangements. These details are confidential, may be misused and could lead to a serious breach of security.

Staff and contractors are ultimately responsible for their own online behaviours. They must take care to avoid online content or actions that are inaccurate, libellous, defamatory, harassment, threatening or may otherwise be illegal. It is possible for staff or contractors to be subject to civil proceedings or criminal prosecution. Remember; once something is put on a social networking site even if you delete it, there may be a record of it kept indefinitely.

Note: These guidelines apply to all methods of accessing social networks. This includes organisation-owned or personal computers, any mobile devices, etc.

18.0 Safe Haven Procedures - Sending Person Confidential Data or Commercially Sensitive data

Safe Haven is a term used to describe either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure person confidential data (PCD) or commercially sensitive information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by post, fax or other means.

If such information needs to be sent inside or outside of the organisation by post or fax, the Safe Haven procedures outlined in this document must be followed.

The principles can equally be applied to ensure the secure transfer of business confidential information.

Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

Before sending any PCD or commercially sensitive information, it should be considered whether it would be sufficient to send anonymised or pseudonymised information instead.

Information that is ‘lost’ or ‘missing in transit’ in any format should be reported as an incident as detailed in the “**Information Governance Incidents**” section of this handbook.

Pseudonymisation

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual. Pseudonymisation is defined with the UK GDPR as “the processing of personal data in such a way that the data can no longer be associated with a specific data subject without the use of additional information.” This may involve replacing names or other identifiers which are associated to individuals, for example, a reference number.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

ICB/CSU Business Intelligence (BI) Teams use analytic tools to supply the ICB with pseudonymised reporting data to enable the ICB to monitor, forecast activity, spend, performance, outcomes and benchmarking. All requests for pseudonymised data should go through the appropriate BI team if you do not have a legal basis to access the identifiable data.

Safe Haven Email Procedures

When sending emails containing PCD or commercially sensitive information, the email must be sent to and from an nhs.net account.

For the latest NHS Digital guidance can be found at

<https://digital.nhs.uk/services/nhsmail/guidance-for-sending-secure-email>

Contact the IG Hub if you are unsure whether an account is secure if not covered above.

18.1 NHS Mail Encryption Facility

NHS.net users can securely share sensitive information with non-accredited or non-secure email services, for example those ending in.nhs.uk, Hotmail, Gmail and Yahoo.

The new NHS.net encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors.

NOTE: It is not possible for anyone other than an NHS.net user to initiate an encrypted email exchange using the NHS mail encryption feature, however by replying to an encrypted email received from an NHS.net email address, the encryption is maintained.

If you have a contact that uses a non-accredited or non-secure email service (e.g. ending .nhs.uk) with whom you need to exchange sensitive information, you will need to send the initial encrypted email that they can then open, read and reply to securely. Guidance on how to do so has been published by NHSmail and can be found at <https://portal.nhs.net/Help/policyandguidance>

18.2 Safe Haven Post Procedures

Important points to note when sending PCD or commercially sensitive information by post:

- Never use internal envelopes or previously used envelopes.
- Whether being sent internally or externally, the information must always be tracked. When sending externally, it is advised that the information be sent by a tracked delivery method (e.g. recorded delivery or special delivery)

This can be done by using either a tracking system or post book. The following information must be included as a minimum:

- Date the information is being sent
- Method of sending, i.e. internal, recorded delivery, 1st class, etc.
- What information is being sent

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Where the information is being sent to
- Initials of the person responsible for sending the information
- Request that the recipient confirms receipt

18.3 Internal Post Procedures

When sending PCD or commercially sensitive information in the internal post system the following procedures must be followed at all times:

Secure Bag**:

- Log all items which are being sent, stating where it is going to, date sent; secure bag number and the signature of the person packaging the information
- Ensure that the secure bag is numbered, and the information is placed inside along with a compliment slip or memo, requesting that the recipient calls to confirm receipt
- Ensure that the contents of the bag are correct before sealing
- Seal the bag, using an appropriate seal
- Address the bag to a named individual only (specific job title where not possible), including full postal address. Also include a return address
- Place into the internal mail ready for sending
- Request that the recipient confirms receipt

**Secure bags are the recommended way to send PCD in the internal mail. The secure bags are far more cost effective than standard envelopes and every effort should be made to use this method.

Standard Envelope:

- Log all items which are being sent, stating where it is going to, date sent, and the signature of the person packaging the information
- Place in a new envelope and mark clearly “Private and Confidential”
- Address the envelope to a named individual only (specific job title where not possible) including full postal address. Also include a return address
- Ensure that the contents of the envelope are correct before sealing
- Seal the envelope and place Sellotape over the seal. Sign or initial diagonally over the Sellotape so that the writing can be seen either side of the tape was it to be removed
- Request that the recipient confirms receipt of the letter, either by enclosing a compliment slip or covering note

External Post Procedures

When sending PCD or commercially sensitive information in the external post, the above “Standard Envelope” procedures must be followed at all times. However, it is strongly advised that Tamperproof Envelopes be used rather than a standard envelope.

18.4 Safe Haven Telephone Procedures

When sharing PCD or commercially sensitive information over the telephone, the following procedures must be adhered to at all times:

When receiving calls requesting personal information in particular:

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Verify the identity of the caller
- Ask the reason for the request
- Ensure that the caller is entitled to the information that they are requesting – if in doubt, take advice from your manager or the Information Governance Team
- If speaking to a service user, ask questions that require them to provide information, rather than giving them details which they need to confirm, e.g. ask them for their address, rather than telling them what is on their record and asking if it is correct
- If you need to pause the call for any reason, remember to use “hold” to ensure the caller can’t overhear other confidential conversations that may be going on in the background
- When calling back, call the main switchboard and ask to be put through. Do not call back to direct numbers or mobile phones
- Ensure that you cannot be overheard when providing personal information
- Ensure that you do not leave any person identifiable information on answer machines/voicemail.

18.5 Safe Haven Room Requirements

If confidential information is to be received in a specific location:

- It should be to a room/area that is lockable or accessible via a coded keypad known only to authorised staff. The code should be changed regularly or in the case of a suspected or actual breach.
- The room/area should be sited in such a way that only authorised staff can enter that location i.e. it is not an area which is readily accessible to all members of staff working in the same building or office, or to visitors.
- If the room/area is on the ground floor, any windows should have locks on them.
- The room/area should conform to health and safety requirements in terms of fire, flood, theft, or environmental damage.
- Manual paper records containing personal information should be stored in locked cabinets when not in use.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.

Please contact the Information Governance team for advice on whether a room can be designated as a Safe Haven.

18.6 Safe Haven Room Procedures

- A list of staff authorised to enter the Safe Haven room must be maintained. Those staff listed will need to be authorised by the Caldicott Guardian for the organisation.
- Only staff named on the above list should be provided with either the key code, swipe card or key to the Safe Haven room.
- No-one who is not listed should be provided with access to the Safe Haven room, under any circumstances.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Should anyone be required to have access to the room for either data quality or audit purposes etc., those people should also be approved and included on the list of authorised staff.
- The door to the Safe Haven room should always be kept locked, even when the room is in use.
- No person identifiable information should be left in trays or on desks when not in use and should be locked away in suitable storage.
- Any computers within the Safe Haven room should be positioned facing away from the door or any windows. Computer screens should be locked immediately and not wait until the screensaver appears.

19.0 Email

19.1 Email Retention

There is occasionally a misconception that email messages constitute a short-lived form of communication. All email messages are subject to Data Protection and Freedom of Information legislation and can form part of the corporate record. Emails should be retained in line with the retention schedule set out in the Records Management Code of Practice for Health and Social Care 2021 with the retention period being determined by the content/subject of the email.

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

Emails should not routinely be saved to shared drives or other shared storage areas unless there is a genuine need for the content to be accessible to others, for example if the email contains guidance or instructions that are applicable to a whole team.

MS Outlook should not be used as a final storage system. If the email or associated attachment refers to something "official" such as a decision, an action, or contract then it has a retention period and should be stored appropriately with the ICB's secure drive. Storage location will be department specific - shared drives for those who need to see it, but if it was a HR issue for example it would only be suitable for it to be shared with specific people.

As attachments within emails, don't always save when an email is saved so best practice would again be to save them with the downloaded email and with appropriate naming so the two elements can be associated to each. These again, should only be accessible to appropriate persons.

19.2 Dos and Don'ts of Email

Users may not use the organisations email systems:

- To breach copyright or intellectual property rights of a third party
- To view, store, download, send, forward or copy inappropriate material. Examples include but are not limited to; obscene or pornographic material, discriminatory material or anything of a criminal nature
- To send defamatory or libellous messages
- To breach the UK GDPR/DPA18

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- To forward chain or junk email

In addition, the use of a non-NHS email account (personal or web mail) is not permitted for the purpose of the organisations business under any circumstances.

Personal use of the organisations email system is not permitted where it substitutes for a webmail system such as Gmail.

The organisation considers email as an important means of communication and recognises the importance of appropriate email content and prompt replies in conveying a professional image and delivering good customer service.

The organisation requires all users to adhere to the following guidelines:

- Write well-structured e-mails.
- Use short, descriptive subjects.
- Signatures must adhere to the corporate standard,
- Do not send unnecessary attachments.
- Before opening email attachments, ensure that you are satisfied of the validity of the sender and the attachment.
- Ensure that the purpose and content of the e-mail message is clearly explained.
- Do not write emails in capitals. This can be considered rude and aggressive.
- Use a spell checker before emails are sent.
- If you require a response by a specific date, make the recipient aware of this deadline.
- Only mark emails as important or high priority if there is a genuine need to.
- Ensure emails are only sent to people who need to see them and only use the reply to all button when necessary.
- Email should be treated like any other correspondence and should be answered as quickly as possible.
- When on annual leave or away from the office for over one day, the Out of Office facility should be used.
- Ensure that the content is verifiable, evidence based and capable of being subjected to public scrutiny, including applications made under the Freedom of Information Act 2000 and the Data Protection Act 2018;
- Be responsible about your use of email; be aware that the email you send may be forwarded without your prior knowledge or consent, or you may be sending to a recipient who has shared access to their inbox with another member of staff, for example their PA;
- Make a clear distinction between opinion and fact.
- Always check the recipients email address is correct before sending.
- 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.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

19.3 Sending emails to mailing/distribution lists

If an email is to be sent to a number of people or to the members of a mailing/distribution list, it may be that the recipients do not (or should not) know who else the email has been sent to, particularly if the recipients include members of the public. Therefore the “BCC” field should be used rather than the “To” or “CC” field to allow the email addresses of the other recipients to be concealed.

This means that the recipient list of the email cannot be reused, and it reduces the chances that the recipients will receive spam or viruses as a result of having shared their email address with many others.

Alternatively, it may be advisable to set up a distribution list and use the alias rather than including individual names or email addresses in the headers.

19.4 Recalling emails

If an email has been sent in error, for example to an incorrect recipient or an attachment has been missed off, it may be possible to recall the email. However, please note that messages must be recalled as soon as possible because this function will not work if the recipient has already read the email. Also, the recipient of the email that you want to recall must also be using an Exchange account, not a webmail account such as Gmail or the recall won't work.

To do this, open the sent email that is to be recalled and select **FILE** in the left-hand corner. Click on “Message Resend or Recall” Then click on Recall message. You will then have the option to either delete the message or replace it with a new message.

19.5 Monitoring

At the request of the Chief Executive Officer the IT service may carry out investigations into email usage.

All external emails are routinely virus scanned and where viruses are detected the email is quarantined until clean. If this is impossible then the email administrator will contact the recipient.

Formal complaints about the misuse of email will be investigated and managed according to the organisations existing grievance and disciplinary policies. Inappropriate emails will be automatically blocked for the protection of the organisation and individuals (e.g. spam and adult content).

Section 6 of the Regulation of Interception of Communications & Provision of Communication-Related Information Act of 2002 (RICA) allows companies to monitor and intercept email provided that it takes place “in the course of the carrying on of any business” at the company.

The ICB may therefore open e-mails in an absent employee's inbox if this is necessary to see whether there are business communications that need to be dealt with in the employee's absence. However, the company must not open e-mails that in their unopened state appear not to relate to the business (for example e-mails that are marked “personal” in the header) unless there are convincing grounds on which

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

to believe they are in fact business related. This does not prevent an interception which is carried out only to gain access to the contents of business communications, but which may incidentally and unavoidably involve some access to other personal communications on the system.

Due to this Act, should there be a necessity for an employee to use their work email for personal emails, it is recommended that they put 'PERSONAL' in the subject line of the email, for example, or create rules in Outlook that moves all incoming personal messages to a separate folder, therefore meaning that should their emails need to be accessed, for example while they are on leave or off sick, then work emails can be distinguished from personal without actually opening the message.

If work email accounts are used for personal emails, then once the email is on the organisations network, it becomes the responsibility of the organisation to protect it under the UK GDPR/DPA18.

For this reason, a process has been put in place to ensure that access to staff emails is suitably protected so that the messages can be accessed only with a valid reason. A request for access to another user's emails should be made through the Information Governance team.

19.6 Long Term Absence

If a staff member is on long term absence (more than four weeks), their line manager should, with the help of the IT Service, redirect their email account to someone else within the department to manage the account. The justification of redirecting the messages should be clearly established prior to redirection. The duty of confidentiality should be impressed upon the member of staff who receives the redirected mail.

It must also be ensured that an out of office message is added to the account at the earliest opportunity. It is recommended that it is set up so that an automated response is sent to every email, rather than just the initial email received from a sender.

19.7 Shared Email Access

There may be circumstances where there is a requirement, for example, for a PA to access a Director's email account.

Under no circumstances should this be facilitated by the Director sharing their network account password with their PA. Doing so is a breach of policy and must be reported as an incident via the incident reporting process.

Microsoft Outlook provides the facility for a user to share their inbox with other users in the same way as a calendar can be shared. Other items such as contacts or tasks can also be shared in this way.

It should be noted that where access is granted to another user, that user may have access to any private, confidential or sensitive materials associated with the respective user account. As a result, access should ONLY be authorised

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

where this is absolutely necessary for operational purposes (and preferably with the individual’s consent). Access can be “tailored” by applying rules within your inbox. For example, a rule could be set up which moves any items received which are marked as confidential to a subfolder rather than leaving them in your main inbox. Please refer to the above section “Monitoring”.

Any person, who is granted access to another user’s inbox to fulfil the requirements of their role, should only view the information required to allow them to do so. Users accessing inboxes of other staff are required to treat all material viewed as confidential and not to act upon it or disclose it to any other person except those directly associated with the operational requirement for which the access was granted. They must preserve the confidentiality of any private or personal data that they may view inadvertently whilst undertaking operational matters.

If you need to share your complete inbox, including any sub folders, with another user then this needs to be facilitated by the IT Service and so a call must be logged with your IT Helpdesk. When doing so, please be mindful that this will mean that ALL emails will therefore be accessible to the user with whom you share your inbox.

19.8 Accessing another user’s inbox via the IT Service

If it is not possible or appropriate to request a user share their inbox with you, for example because they are absent from work, have left the organisation or the access is required for a HR investigation, then a request must be made to the IT Service, via the Information Governance team.

20.0 Video and Teleconferencing via Microsoft Teams

Video and teleconferencing are becoming a powerful way for colleagues to communicate and collaborate but can be open to abuse both deliberate and accidental as systems are designed to be easy to use with the ensuing security relying more and more on end users than on restrictions built into the software/hardware. When using video conferencing i.e. Teams please make sure that you are aware of who is on the call/ meeting.

Extra care and precaution should be exercised whilst sharing your screens or conducting a training session. It is best practice to close all screens that you do not need for the meeting/ training session to ensure that the incorrect screen is not shared.

The use of such equipment will also contribute to the organisation’s ability to reduce the need for travel.

As this form of communication is two-way technology, equipment should be located and used where there is the least risk of private activities being accidentally seen or overheard.

When arranging the meeting, and sending out invites, this guidance should be included to ensure that all participants are aware of and signed up to the following:

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- All participants must identify themselves at the beginning of the meeting and when speaking, to ensure that the other participants are aware of the speaker.
- No recording outside of that organised by the Chair shall be made.
- No participants shall be expected to invite others to take part in the meeting/session without the express consent of the Chair.
- Headsets should be worn for all meetings/sessions where participants may be overheard by others, and webcams should be used where they cannot be overseen by others outside of the invited participants.
- Where a participant enters/leaves the session, whilst it is in progress, the Chair must ensure that all participants are aware of the fact, with participants announcing their arrival/leaving with their name and job role etc.
- At the end of the session the Chair must make sure that all participants are aware that the session has concluded, and if a recording is being made that the recording is stopped at this time.

21.0 Responsibilities

21.1 Chair of Meeting/Session

The Chair is responsible for the overall running of the meeting/session. They must ensure that all participants are introduced at the beginning of the meeting/session, and that they are all able to see and hear each other. The Chair will be responsible for ensuring that reasonable adjustments are put in place where a participant has an access need.

They will be responsible for the facility itself for the duration of the meeting/session, from ensuring all is in order before the meeting, coordinating with IT Technical Staff if required, and ensuring all is in order at the end of the meeting.

All participants invited to the meeting/session should be aware as to whether the meeting/session is being recorded or not. They should also ensure that no additional recordings are made by participants themselves.

If the session is recorded, the Chair is responsible for ensuring that all participants have given their consent and that there is a verbatim copy available for all participants if requested.

21.2 Meeting/Session Participants

All participants are expected to adhere to this guidance and return the signed “Compliance” forms that they are given, either at a training session or before their first video or teleconferencing meeting/session.

No additional recordings are to be made without the express permission of the Chair before the meeting/session commences.

Headsets must be worn to ensure that their conversations are not overheard, and any webcams used should not be overseen by others where possible and backgrounds should be blurred.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

21.3 Training & Implementation

Guidance on the use of MS Teams is available to ICB staff, all users need to familiarise themselves with this guidance before using the system or other video conferencing technology.

22.0 Data Security and Protection Incidents

It is important that information remains safe, secure and confidential at all times.

All staff are encouraged to report all incidents via the Incident Reporting Form /Datix Incident Reporting system as soon as is possible following the identification of the incident.

In addition to the internal reporting of incidents, it is a legal obligation under UK GDPR/DPA18 to notify personal data breaches to the ICO within 72 hours, unless it is unlikely to result in a risk to the rights and freedoms of an individual.

All health and social care organisations are to use the reporting tool accessed via the new Data Security and Protection Toolkit to report data breaches. This reporting will be undertaken by the Information Governance Team.

22.1 What is a data breach?

A data breach, as defined under UK GDPR/DPA18, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, personal data transmitted, stored or otherwise processed.

(Personal data is defined as: 'any information relating to an identified or identifiable individual')

22.2 What are the types of breaches?

UK GDPR/DPA18 defines three types of breaches: Confidentiality, Integrity or Availability.

- Confidentiality breach – unauthorised or accidental disclosure of, or access to personal data
- Availability breach – unauthorised or accidental loss of access to, or destruction of, personal data
- Integrity breach – unauthorised or accidental alteration of personal data

What is a Data Breach?

Breach of Confidentiality - A data breach, as defined under UK GDPR/DPA18, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to, personal data transmitted, stored, or otherwise processed.

(Personal data is defined as: 'any information relating to an identified or identifiable individual')

Breach of Process – Where a process has not been followed but no identifiable information has been disclosed.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

22.3 Breach Reporting Process

1. Inform the CSU IG Team and line-manager within 24 hours of becoming aware of a near miss, breach, or potential breach.

IG Team

Email: mlcsu.ig@nhs.net

Tel: 01782 872648

CSU IG Team to contact the reporter at their earliest opportunity to obtain the following information

<p>What has happened? Include details as much as you can about what happened including:</p>	
<p>Name and job role of the person who has caused the breach, which team are they in and which organisation are they employed by?</p>	
<p>What information has been breached, i.e., name, address, full CHC record etc? This needs to be specific, including if any particularly sensitive data such as sexual health, mental health, safeguarding data etc.</p>	
<p>Did the information contain any personal data about any other data subjects, next of kin for example?</p>	
<p>How did the breach occur?</p>	
<p>Where has the information gone?</p>	
<p>How was the information sent, i.e., post, email etc and please state if this was a secure encrypted method if known?</p>	

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Has it been accessed and seen by someone inappropriately?	
Has the information been returned, double deleted, or otherwise securely destroyed and not further saved used or shared? If not, this should be done immediately, and actions confirmed by recipient.	
If relevant, has the information now been sent to the correct recipient?	
If the information were pseudonymised (i.e., data subjects initials or NHS number, patient ID etc) could the recipient identify the individual, for example using a system they currently access? If they can identify the individual is that because they have a legal basis (within their job role) to have the information, but it was not sent using the correct process?	
How did you find out, how did you become aware?	
When did you become aware? date and time	
Was the incident caused by a problem with a network or an information error? (This could be a technical or system error).	
What is the local ID for the incident?	To be determined by IG
Who is the data controller? (Note, it can only be the CSU IF the data subject is a CSU member of staff). Otherwise, it must be an ICB. The data controller is the organisation who controls how the information of the data subject is	

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

processed. CHC always process patient data on behalf of an ICB, therefore that ICB would be the data controller.	
When did the incident start? (This is when the breach actually occurred.)	
Is it still ongoing? (Is the information still at risk or has it been fully mitigated). Yes or no	
When did the incident end? (When was the breach fully mitigated?) Date the incident stopped	
Have the data subjects been informed? Yes/no/planned – to be decided by the Caldicott Guardian	
Does the incident impact across a national border? Yes or No	
If yes, have you notified overseas authorities? Yes or No	
Have you informed the Police? Yes or No	
Have you informed any other regulatory bodies about the incident? i.e., GMC, H&SE CQC. If yes, who and reference number If yes, who?	
Has there been any media coverage that you are aware of? Yes or No	

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

<p>What other actions have already taken place or are planned? (What have you already done to mitigate the breach and what are you planning to do? This could include requesting the information is returned or securely destroyed).</p>	
<p>How many citizens affected? (How many data subjects' information have been breached. This could include next of kin information on a letter regarding a patient).</p>	
<p>Who is affected, i.e., children, vulnerable adults, staff, patients, next of kin? (Please consider if the information breached contains any personal data about other data subjects, next of kin for example)</p>	

When scoring the breach below, it is important to be conscious of the type of information that has been breached, who is affected and who has inappropriately accessed the information. Could this have an impact on the data subject and if so, how big an impact? How likely is it that the impact will actually occur?

<p>What is the likelihood that individuals' rights have been affected?</p>	<p>Not occurred</p>	<p>There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence</p>	<p>Yes or No</p>
	<p>Not likely</p>	<p>In cases where there is no evidence that can prove that no adverse effect has occurred.</p>	<p>Yes or No</p>

<p>Document Owner:</p>	<p>Approval date:</p>	<p>First published:</p>
	<p>Next review date:</p>	<p>Version: Final</p>

	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.	Yes or No
	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.	Yes or No
	Occurred	There is a reported occurrence of an adverse effect arising from the breach.	Yes or No
What is the severity of the adverse effect, none, potential, some effect, pain, suffering, financial or death?	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach	Yes or No
	Potentially some minor adverse effect or any breach involving vulnerable groups even if no adverse effect occurred	A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.	Yes or No
	Potentially Some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled	Yes or No

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

		procedure that has the potential of prolonging suffering but does not lead to a decline in health	
	Serious - potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.	Yes or No
	Death / catastrophic event	A person dies or suffers a catastrophic occurrence	Yes or No

These questions are all subjective depending on the breach itself. Some of the questions may not be relevant depending on some of the other answers.

2. Reporter to return the answers to the CSU IG Team, copying in Line-Manager within 24 hours
3. CSU IG Team to log the breach, this will generate a CMS number which is to be used in all further correspondence
4. CSU IG Team to inform the reporter and the line-manager of any immediate action needed to be taken
5. CSU IG Team to inform the SIRO of the breach
6. CSU IG Team to report the breach on the DSP Toolkit if authorised by the SIRO

NOTE: The DSP Toolkit will establish if the breach is reportable to the Information Commissioner Office (ICO) and full RCA is needed

If the breach is non-reportable, a full RCA is unlikely to be needed but the IG Team will liaise with the reporter to complete a short form RCA with recommendations. If the breach is reportable, the RCA must be sufficient to meet ICO requirements. The SIRO is responsible for notifying the Board of all reportable breaches.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

22.4 Investigation Process

NOTE: The Investigation process is to establish what happened and what can immediately be done to mitigate the consequences of the breach.

- The CSU IG Team will undertake an investigation alongside the ICBs

Full Root Cause Analysis (RCA)

NOTE: The Root Cause Analysis (RCA) process is to establish what caused the breach to happen and develop actions to prevent similar breaches occurring again.

1. CSU IG Team to discuss with the line-manager of the reporter, and the IG Lead for the ICBs, who should be appointed as the lead for the RCA
2. The CSU IG Team to liaise with the RCA lead as to how to establish the root cause of the breach Once completed, the CSU IG team to develop a list of recommendations which will be send to the SIRO, DPO, CG, IG Lead, IG BPs, and manager of the team
3. Manager of the team/RCA Lead to present their actions and outcomes to the IG steering group
4. Caldicott Guardian to work with CSU IG Team to determine whether the data subject should be informed where the breach involves identifiable information

The RCA should include:

1. Breach description
2. Pre-investigation risk assessment
3. Background and context of the breach
4. Information and evidence gathered
5. Report Limitations (as appropriate)
6. Chronology of events

When is an incident reportable under UK GDPR/DPA18?

Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation.

The **significance** is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest.

The **likelihood** of the consequences occurring are graded on a scale of 1-5 1 being a non-occurrence and 5 indicating that it has occurred.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Grade the potential significance of the adverse effect on individuals

1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially Some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Establish the likelihood that adverse effect has occurred

1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Both the adverse effect and likelihood values form part of the breach assessment grid.

There are a limited number of circumstances where even when an organisation is aware of a breach of personal data there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances notification may not be necessary.

- encryption – Where the personal data is protected by means of encryption
- ‘trusted’ partner - where the personal data is recovered from a trusted partner organisation
- cancel the effect of a breach - where the controller is able to null the effect of any personal data breach

*trusted’ partner – breach contained, sent to wrong department for example, but where recipient may be considered trusted not to read or access data sent in error and to comply with instructions to return it.

22.5 Breach Assessment Grid

The operates of a 5 x 5 basis with anything other than “green breaches” being reportable. **Incidents where the grading results is in the red are advised to notify within 24 hours.**

Impact	Catastrophic	5	5	10	15 20 25 Reportable to the ICO DHSC Notified		
	Serious	4	4 No Impact has occurred	8 An impact is unlikely	12	16	20
	Adverse	3	3	6	9 12 15 Reportable to the ICO		
	Minor	2	2	4	6	8	10
	No Impact	1	1 2 3 4 5 No Impact has occurred				
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				

60

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

22.6 Sensitivity Factors

Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following it must still be reported as a level 2 and as such notifiable to the ICO.

If a breach involves certain categories of vulnerable groups, it must be scored as a minimum 2 on both axes of the scoring matrix although it may be higher depending on the severity or likelihood but will not in all circumstances be notified to the ICO.

For clarity special categories under UK GDPR/DPA18 not listed below include;

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

For clarity Special Categories of personal data under UK GDPR/DPA18 are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- and the processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

22.7 Assessing risk to the rights and freedoms of a data subject

UK GDPR/DPA18 gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following;

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Depending on the outcome of the scoring matrix the risk may be high risk and be significant enough to notify to the ICO.

If there is any doubt that a breach is significant enough for notification, or there is any uncertainty then it is always best to contact the Information Governance team at the earliest opportunity.

23.0 Records Management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal and destruction.

Any information held is only of use if it can be retrieved easily and the data contained within it is accurate and up to date.

It is important that the organisation knows what information it holds, how it is stored and accessed so that it can fulfil its legal requirements as well as being efficient and effective in its day to day activities.

Information contained within corporate records may be required to meet the requirements of legislation such as the Freedom of Information Act (2000) and The Environmental Information Regulations (2004) and as such must be accessible to ensure that the specific time limits set out within the legislation is met.

Clinical records and other personal data may be required to meet the requirements of legislation such as the Access to Health Records Act (1990) and UK GDPR/DPA18 to fulfil subject access requests.

The organisation appoints Information Asset Owners and Information Asset Assistants to maintain a register of the organisation's Information Assets and record how the information is used, to ensure that any associated risks can be managed.

Staff must feel confident that they know how to access and store information in order for them to carry out their role to the best of their ability.

Identification/Naming of Records

All records should be clearly identifiable from the file name or from the file cover. It should include an accurate title or description of the information contained and where appropriate the department or service to which it relates.

Naming of electronic records

File Names are the names that are listed in the computer's file directory and that are allocated to new files as they are saved for the first time. By naming records consistently, this will enable staff to distinguish similar records at a glance.

Naming records according to an agreed convention will make naming easier for staff as a "re-think" process will not be required on every occasion.

A file title should be:

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- descriptive- it says what the document is about and accurately reflects the contents.
- helpful- it distinguishes the document from others on the same/ similar topic.
- consistent – it follows the conventions set down by the organisation.

Documents should always contain the following elements:

- date
- subject
- document type
- version or status

Naming conventions

- Keep file names short but meaningful- avoid use of personal names (e.g. Staff names should not be used as file names i.e. BOB SMITH or BOBS FOLDER) and abbreviations and codes that are not commonly understood or may not be in the future;
- Make sure documents can be identified on their own without the folder in which they are saved, e.g. Audits\2013-14\2015-09-20 Audit report on.....
- When including a number in a file name always give it as a two-digit number, i.e. 01-99 (unless it is a number with more than two digits).
- Dates should always follow the BS ISO 8601:2004 format, YYYY-MM-DD, to ensure documents are stored in chronological order.
- When adding personal names, always put the Surname first (e.g. Smith B).
- Avoid using common words such as ‘drafts’ or ‘letters’ at the start of file names unless it will assist with record retrieval.
- Make sure elements in the file title are ordered in the most appropriate way to retrieve the record. This will depend on the audience e.g. minutes may be retrieved by date so the date element will appear first, whereas policies might be retrieved by the description so this will come before the date.
- A folder name should not be replicated to subfolders within the file (i.e. Audits\ 2010-2011 rather than Audits\ Audits 2010-2011\).
- Correspondence record titles should always include the following elements: name of correspondent, subject description (if not already in folder name), date of letter, email etc. and ‘rcvd’ if incoming correspondence.
- Avoid use of non-alphanumeric characters in file names (i.e. * : / \ < > “ ! + = £ \$ & ,).
- Do not use the document creator’s name in the title unless this information genuinely adds to a description of the content (e.g. in correspondence). This information can be added directly in the document or accessed in the document or folder’s Properties.
- It is better to use a job title rather than the name of the person in the title of a folder or file and it is best to provide the job title in full rather than use an acronym.
- Include a version to the file name for documents which are subject to changes being made e.g. policies and procedure, (see Version Control section below for more information).

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Naming of paper records

The organisation will follow the advice and recommendations issued by The National Archives, i.e.:

- Give a unique name to each record.
- Give a meaningful name which closely reflects the record content:
- Express elements of the name in a structured and predictable order.
- Locate the most specific information at the beginning of the documentation name and the most general information at the end.
- Give a similarly structured and worded name to records which are or can be linked (e.g. an earlier or later version).
- Include a version in the title of records which are subject to changes being made e.g. policies and procedures (see Version Control section below for more information).

Version Control

For all records created, version control is important as documents undergo revision and updating on a regular basis. Version control should be used to manage revisions of a document, enabling the reader to differentiate one version of a document from another. It is particularly important as version control should also be used to clearly identify a final version of a document, which will then assist with referencing and, when required, off-site storage.

Most documentation will require the use of simple version control techniques such as the use of naming conventions and version numbering to distinguish one version from another. It is recommended that this practice is used for all documentation where more than one version exists.

Use of numbering within version control should be used to reflect major changes from minor (i.e. whilst in development, version control should be version 0.1, each subsequent set of amendments to the document after that should increase the last digit by 1- e.g.0.1 then 0.2, 0.3 etc. The file name could also reflect its 'draft' status.

Once there is a final approved version, this will be named 1.0, and any subsequent draft amendments should be saved as version 1.1, 1.2 etc. If further approval is required, it will become version 2.0 and so on). The version number and date should be clearly visible within the document, such as the front cover with the version number being contained within the footer of the document to ensure that it is visible on every page. Final versions could include the word 'final' as part of the file name.

Classification

Both electronic and paper records and documentation may require classification. Records can be classified into categories. All NHS documents will be classified as OFFICIAL with the subcategories of OFFICIAL- SENSITIVE: COMMERCIAL and OFFICIAL- SENSITIVE: PERSONAL. If one of the two OFFICIAL- SENSITIVE categories is appropriate, consideration must be made in relation to the retention, storage and dissemination of this information. Staff must also be aware that records classified as OFFICIAL- SENSITIVE within the organisation may also on occasion be

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

accessible to the public under legislation such as the Freedom of Information Act 2000.

Storage of Records

Electronic records storage

Electronic documents that contain information that supports a decision-making process of any description, undertaken by any directorate/department or service must be managed to the same standards expected of paper records and for this reason, they must be retained on a corporate shared drive or appropriate intranet site.

All work-related files (documents, spreadsheets, etc.) must be stored on the shared network and data that is for your personal use only is stored on your personal drive (you may know this as “My Documents”, U Drive, I Drive etc.).

The disk capacity for the storage of files is limited. It is not permitted to save music files or digital images from personal cameras to the network. The IT Service reserves the right to delete such files without notice.

Access to folders on the shared drive should be restricted, based upon the user’s employment position and requirement under that post to access information.

The organisation should use a clear and logical filing structure for electronic records to support the retrieval and retention of the records. This may reflect the way in which paper records are stored where appropriate to ensure consistency. Alternatively, the names allocated to files and folders should be done in a way that allows intuitive filing.

Paper records storage

Good quality documentation standards are essential to provide accurate records of the organisation’s activities.

Filing

Records and documentation contained within a paper file or filing system should be securely fastened using treasury tags and folder ties appropriate to the record type. Loose papers and plastic wallets should be securely fastened as loose documentation even if placed in a plastic wallet can be easily lost, misplaced or damaged. The use of Sellotape and staples to secure paper and documents into files is not recommended (staples can be used to staple a document together, but not as a method as a secure file fastening.)

Storage requirements

Records should be retained in facilities appropriate to the record type (i.e. confidential information should not be retained on open shelves in open office areas), environmental considerations such as excessive lighting, damp or flooding must also be considered when decisions are made for the housing of records in the work area. Record storage facilities should not be overcrowded and should allow for easy retrieval and return of records.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

The papers and documentation contained within records should be arranged and retained in a logical manner, which has structure and is ordered by chronology.

Duplicate documentation should be removed where possible. When a file becomes too large or excessive a second volume should be created and indexing, and version control used.

Directorates, Departments and Service Areas should record all record types on the Information Asset Register. This will be used by the organisation as a file plan which will be used for the auditing of records.

Records should be stored securely and not left unattended or accessible to staff who are not authorised to access them. Where records are removed from the work area a tracking system should be used. (See section below- Tracking and Tracing of Paper records for more information.)

Indexing

An index (or register) should be used primarily to signpost staff to the location where paper records are retained (i.e. the relevant folder or file within a filing cabinet), however, it can also be used by staff to identify the information contained within those records. An index should be developed to be a user-friendly structure to aid staff in the easy location and retrieval of records and documentation. (It is not recommended that staff file or retain records in desk drawers as this limits accessibility and may lead to issues with version control as well as record naming and indexing or continuity of patient care). It is requested that all records are retained in central filing systems ensuring accessibility to all appropriate staff as and when required.

Usage/Transfer of records

Access

Access to the shared drive should be managed to ensure that access to the information contained electronically is controlled in the same way as paper documents. This should be done by restricting folders to staff groups and not by password protecting individual documents as this may make them inaccessible in the future should the password be forgotten. Even the IT Service will be unable to remove passwords from Microsoft documents.

Tracking should also take place to ensure that the cross-referencing of electronic records with their paper counterparts can take place and be relied upon that version control is maintained both electronically and in paper format.

Tracking and Tracing of paper records

Records are created and captured in order to be used; therefore, record keeping systems must include effective mechanisms for tracking and tracing their whereabouts and use. Effective procedures must be in place to ensure swift retrieval, an audit trail of use and for their accurate return.

A comprehensive tracking system should include:

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- Effective aides to identify documents and records and provide the location details and highlight any restrictions appropriate to it
- The use of tracer cards and a register to track records that have been accessed and relocated

Depending on the nature of the document/record, authorisation for access may be required. Where most records are available to the public an authorisation procedure is not necessary. However, where records are sensitive due to data protection, commercial confidentiality or security issues, these documents and records will need to be tracked and monitored to ensure that appropriate authorisation processes are in place to approve staff access.

Effective tracking will ensure that records can always be located when required and that records remain controlled and secure, thus enhancing their reliability and authenticity.

As a minimum, a tracking system should include:

- The record reference or unique identifier
- Title or description of the record
- The individual (including job title, telephone number and e-mail address), department and location accessing the record
- Date and signature confirming removal and return of record

Tracking systems ensure records are appropriately tracked when records are sent between staff/departments. However, if a record is being permanently transferred, please contact the IG team for this document.

Procedure for the secure movement of records during team relocation

It is a business need that from time to time, teams and departments will be required to ‘relocate’ from one premise to another. It is during these times that the organisation is at its highest risk of losing records. For this reason, it is important that there is a clear procedure for staff to follow to ensure the secure movement of organisational records. This procedure relates to the movement of **ALL** organisational records.

Due to the nature of the procedure, it can be assumed that on most occasions, teams will be moving a high number of records. As anything over 50 records is classed by the Department of Health as a ‘bulk’ removal of records then there is a greater level of security that must be applied to those records in transit.

Scope of the procedure

This protocol covers any work carried out by moving contractors, whilst under contract with the ICB. This also includes the expectations and responsibilities placed upon staff, working for the contracted companies, who will be moving the records.

Any records removed shall be in sealed containers and access to those records will not be provided. Therefore, this will not be an information sharing agreement but will instead be an agreement between the ICB and the contractors undertaking the relocation of the records to ensure the secure removal of records.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

The responsibility for ensuring the security of records during moves lies with the service area concerned, not the Information Governance team, the Premises team, or the moving contractors.

Preparing Records to Be Moved

- All records that are to be moved should be recorded on a movement of records listing sheet, the sheet should include the number and range of records included in the box.
- Teams will need to assign each container a unique identifier which should follow the format of **TEAM/DATE OF MOVE/001** for example IG/01.06.15/001.***
- The containers should be clearly marked with its unique identifier. ***
- Once all records have been listed and placed into the container, the list should be checked and countersigned by a colleague to ensure that the records recorded are placed within the container.
- The container should be sealed immediately and not opened until the records reach their destination.
- A list of all the containers should be recorded. This will need to be signed by the person transporting the records.

*****If moving containers are being used then each box should be sealed using two cable ties (1 at each end). The cable ties must contain a unique number – this is the identifying number that will be assigned to that box and should be listed on the movement of records listing sheet.**

Moving the records using an external company

- Sealed containers should be loaded onto the removal van.
- The staff member that has been assigned responsibility for the removal of those records should check all boxes loaded onto the van against the container list and sign to confirm that they are all sealed, intact and loaded onto the van.
- The driver should then complete the same check and sign the container list to confirm that they are taking the responsibility from that point, for the security of those containers and records.
- When the van reaches its destination, the member of staff responsible for those records, should meet the van and perform the following checks:
 - Check that the containers are all sealed
 - Check that there is no damage to any of the containers
 - Check that all boxes that were signed onto the van are present and correct.
 - If all checks are carried out and satisfactory the boxes should be removed from the van and should be signed on the container list as having arrived securely.

Moving the records using staff members vehicles

- Sealed containers should be loaded into the vehicle.
- The staff member that has been assigned responsibility for the removal of those records should check all boxes loaded onto the vehicle against the container list and sign to confirm that they are all sealed, intact and present.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- If the staff member assigned responsibility for the removal of the records is also the driver, then the container list will need to be countersigned by another member of ICB/ CSU staff
- The vehicle should not be left unlocked or unattended at any time once the records have been loaded into the vehicle.
- The vehicle should go directly to the required destination.
- When the vehicle reaches its destination, the member of staff responsible for those records (or if that is the same person as the driver then this action should be completed by the counterperson), should meet the vehicle and perform the following checks:
 - Check that the containers are all sealed
 - Check that there is no damage to any of the containers
 - Check that all boxes that were signed onto the vehicle are present and correct.

If all checks are carried out and satisfactory the boxes should be removed from the vehicle and should be signed on the container list as having arrived securely.

24.0 Retention and Disposal of Records

Disposal is the implementation of a review process, and the term should not be confused with destruction. A review decision may result in the destruction of records but may also result in the transfer of custody of records, or movement of records from one system to another.

Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records consumes time, space and equipment use; therefore, disposal will aid efficiency. Staff members must regularly refer to the Records Management Code of Practice for Health and Social Care 2021– please see the section on retention periods below for more information.

Retaining records unnecessarily may also incur liabilities in respect of the Freedom of Information Act 2000 and the UK Data Protection Act (2018). If the organisation continues to hold information which they do not have a need to keep, they would be liable to disclose it upon request. The UK Data Protection Act (2018) also advises that we should not retain personal data longer than is necessary.

Staff members are recommended to seek specialist advice from the Information Governance team when considering destruction of the organisation’s records through a commercial third party.

Staff members are also recommended to seek specialist advice from the Information Governance Team when considering off-site storage of the organisation’s records with a commercial third party. When inactive records are sent for offsite storage, they must be tracked so that their precise location is known, and an auditable trail of their movement is created.

Short-lived documents such as telephone messages, notes on pads, post-its, e-mail messages etc. do not need to be kept as records. If they are business critical, they

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

should be transferred to a more formal document which should be saved as a record.

Retention periods

All records that are created have an associated retention period. The length of the retention period depends on the type of record and its importance to the business of the organisation and the legal requirements.

All documents and records should be reviewed on an annual basis to ensure that appropriate storage and retention is maintained.

To ensure that all records are retained for the minimum recommended retention period the guidance in the Records Management Code of Practice for Health and Social Care 2021 should be followed:

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf

NHS England have also published guidance which may be more relevant to commissioning organisations that can be used in conjunction with the Records Management NHS Code of Practice. **The NHS England Corporate Records Retention – Disposal Schedule and Guidance** can be found at:

<https://www.england.nhs.uk/publication/corporate-records-retention-disposal-schedule-guidance/>

Disposal

Once records have reached their minimum retention period deadline, they should be reviewed to establish whether there is any justification for keeping them longer e.g. for historical purposes, new episode of care, research needs etc.

If records need to be kept, a decision should be taken whether to keep them as a current record, archive them off site or store them permanently with the National Archives.

For records that have reached their minimum retention period and there is no justification for continuing to hold them, they should be disposed of appropriately.

Paper records of a sensitive, confidential nature should either be shredded using a cross shredder to DIN standard 4 or put in confidential waste that is appropriately destroyed by a company contracted to the organisation. Confidential waste bins should be kept locked and not over filled to ensure information cannot be retrieved from them. Confidential waste bags should be kept in a locked room until collected for disposal.

Electronic records must be deleted from the device and not simply moved into the Trash folder, known as double deleting. De-commissioning of electronic devices such as computers, laptops, notepads, mobile phones etc. should be undertaken according to procedures outlined so that they are completely wiped before being disposed of/destroyed to avoid data being retrievable in the future.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

25.0 Business Continuity Plans

Business Continuity Planning is a method used to identify potential impacts that may threaten the operations of an organisation's business/premises.

The fundamental element of business continuity is to ensure that whatever impacts the organisation it continues to operate.

Business continuity plans will help shape organisational resilience to 'threats', plan counteractions and minimise interruptions to its activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications).

Each team should have Business Continuity Plans in place, and it is the responsibility of members of staff to be aware of the location of plans, and what procedures to follow in the event of potential 'threats' to operations.

For further information regarding Business Continuity Plans, please contact your line manager or the most senior member of staff in your department.

26.0 Digital recording of meetings

The digital recording of meetings as an aide memoir to the minute taker is often required. If the meeting is to be recorded for this purpose, please follow the guidance below:

- There would need to be agreement by all members to audio record the meeting, explaining that this recording would be used purely as an aide-memoire for the minute-taker to ensure an accurate transcript of the meeting.
- Written consent should be obtained from all members agreeing for the meeting to be recorded.
- New Terms of Reference would be required identifying agreement to record the meeting, the reason for recording the meeting, where/who will have the only copy of the audio recording and when the recording will be destroyed.
- The Chair of the meeting has discretion to stop or suspend recording if, in their opinion, continuing to do so would prejudice proceedings at the meeting.
- Prior to the meeting, communications should be sent notifying members that the meeting will be digitally recorded. This should also be identified on the formal agenda.
- All panel members should be advised that the digital recording will be held for:
- The same retention as the written transcription for high/board level meetings, i.e. 3 months
- A minimum of 3 months after the written transcript has been ratified by all members for lower level meetings

The recording should then be destroyed once the above stated retention period has been met.

As the audio recording would be a record for the above agreed time, it is important to record the destruction of this record to assist in audit purposes.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Retention of notes and recordings taken as aide-memoire for a minute taker

For High Level / Board Level meetings; notes and recordings should be retained for the same length of time as the written transcription.

For other lower-level meetings, it is acceptable to destroy notes and recordings 3 months following the written transcript having been ratified by all members of the group.

27.0 Information Risk Assessment and Management Programme

Information and information systems are important corporate assets, and it is essential to take all the necessary steps to ensure that they are always protected, available and accurate to support the operation and continued success of the organisation.

There needs to be a comprehensive programme of activity across the organisation to identify information risks and manage them effectively. From the outset this needs to be recognised as an ongoing activity. A number of key activities in the Information Governance toolkit form the basis of building an information risk framework, namely:

- Mapping flows of information
- Identifying and maintaining a register of all information assets
- Setting out continuity plans for periods of information unavailability

Managing Information Assets

Information assets are identifiable and definable assets owned or contracted by an organisation which are 'valuable' to the business of that organisation, such as:

- databases
- data files
- contracts and agreements
- system documentation
- research information
- user manuals
- training materials
- operational/support procedures
- business continuity plans
- back up plans
- audit trails
- archived information

***Please note that this list is not exhaustive.**

Information assets could be kept in a variety of formats and on a variety of media, e.g. paper, on a shared drive, on removable media (e.g. USB memory sticks, CD-ROM).

Examples of paper assets include:

- patient records
- personnel files
- letters
- referrals

Examples of electronic assets include:

- spreadsheets
- annual leave/sickness records
- local databases
- scanned documents

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- annual leave sheets
- sickness absence returns
- expenses
- electronic copies of letters
- papers for meetings

28.0 Information Asset Register – U-Assure

Information assets may contain **person identifiable** or **commercially sensitive** information.

An Information Risk Management System has been developed which, with the support of the Information Governance team, will allow Information Asset administrators (IAAs) and Information Asset Owners (IAOs) to identify information assets and record details of their content, the security arrangements in place to protect them, and what business continuity arrangements are in place. For each question, a specified range of answers are provided. This approach will allow the information assets to be risk assessed using a standard risk scoring matrix to ensure consistency of risk assessments across the organisation.

Further to this, IAOs are required to assess the worst-case scenario of the possible effects the loss of confidentiality, integrity and availability of each information asset would have to the business, including financial, adverse publicity, relationship with patients or NHS and the risks associated with non-compliance with legislation. This process will assess the business criticality of the asset to allow the organisation's critical assets to be identified, providing the basis of this component of departmental and organisational business continuity plans.

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the information assets held by the organisation and the risks associated with them, resulting in a requirement to review any previously recorded information assets and risk assessments. Consequently, the information asset register should be subject to regular maintenance by IAOs and IAAs, with formal review conducted at least annually. It is essential that whenever new information assets are created, the relevant IAA or IAO is informed, to allow them to create an entry in the Information Asset Register.

This formal review of assets and risk assessments will be conducted at least annually.

28.1 Person Identifiable Data Flow Mapping

In the NHS, numerous transfers of data take place each day. It has long been recognised that this information is more vulnerable to loss or compromise when outside the organisation, i.e. being carried around or sent/copied from one location to another. The requirement to map information flows is a requirement of the DSP Toolkit,

To ensure all transfers are identified, the organisation must determine where, why, how and with whom it exchanges information. This is known as Data Flow Mapping

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

and the comprehensive register provided by this exercise identifies the higher risk areas of information transfers requiring effective management. It also allows any Information Sharing Agreements or contracts that should be in place to be identified.

To adequately protect transfers/flows of information, the organisation must identify the transfers, risk assess the transfer methods and consider the sensitivity of the information being transferred. Transfers of all information (including personal information) must comply with the organisations Safe Haven Procedures (above) and relevant legislation (UK GDPR/DPA18) which requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of, and accidental loss or destruction of, or damage to, personal data).

The loss of personal information will result in adverse incident reports which will not only affect the reputation of the organisation but, in the case of disclosing personal information intentionally or recklessly, is also a criminal offence. With effect from May 2018 fines of up to 17,000,000 pounds or 4% of an organisations total income may be imposed by the Information Commissioner's Office on organisations that do not take reasonable steps to avoid the most serious breaches of UK GDPR/DPA18.

The information recorded in the Information Asset Register allows the identification of all assets of which part or all of their content are sent or received either internally or externally to the organisation. For those assets which are identified as moving in this way, a further module is completed within the Information Risk Management System by the IAA so further information is collected about how and where the information is transferred. This information is then risk assessed to identify areas of high risk and any areas of non-compliance with the organisation's safe haven procedures.

Through this process, the organisation will actively identify and review where person confidential data (PCD) is held, processed or shared to ensure a legal basis for doing so is identified. Where no legal basis can be found an IG breach will be reported and investigated.

As with the Information Asset Register, data flows are subject to change and should therefore be reviewed regularly. A formal review will be conducted annually.

29.0 Data Protection Impact Assessment (DPIA)

A Data Privacy Impact Assessment (DPIA) is a process designed to help an organisation systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of an organisation's accountability obligation under the Data Protection Act 2018, and when done properly helps assess and demonstrate how you comply with all of the organisation's data protection obligations.

It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

DPIA's are a legal requirement, where the processing of personal (including pseudonymised) data is required. The legal responsibility sits with the Data Controller. Failure to carry out a DPIA when required may leave the data controller open to enforcement action including significant fines (£8.7 million or 2% of the total annual worldwide turnover). By considering the risks related to the intended processing before you begin, you also support compliance with another general obligation under Data Protection Act: Data Protection by Design and Default.

In general, consistent use of DPIAs increases the awareness of the privacy and data protections within your organisation. It also ensures that all relevant staff involved in designing projects/services think about privacy at the early stages and adopt a 'data protection by design' approach.

A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate your compliance with all data protection principles and obligations.

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”.

This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR/DPA18 says you must do a DPIA if the plan is to:

- use systematic and extensive profiling with significant effects.
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

The ICO also requires a DPIA if the plan is to:

- use new technologies
- use profiling or special category data to decide on access to services
- profile individuals on a large scale
- process biometric data
- process genetic data
- match data or combine datasets from different sources
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')
- track individuals' location or behaviour
- profile children or target marketing or online services at them
- process data that might endanger the individual's physical health or safety in the event of a security breach

Actions also to be considered

- You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- You must consider the impact on any of an individuals' rights and freedoms, including (but not limited to) privacy rights.
- There are more specific requirements for the content of a DPIA.
- You must seek the advice of the data protection officer in terms of the project meeting the requirements of UK GDPR/DPA 2018. You also need to seek the views of people whose data you intend to process, or their representatives, wherever possible.
- If after doing a DPIA you conclude that there is a high risk and you cannot mitigate that risk, you must contact the IG Team before you can start processing.

The DPO/IG Team can also be contacted for advice on:

- whether a DPIA is required
- how to complete a DPIA
- what measures and safeguards should be considered in order to mitigate risks
- whether a DPIA has been completed correctly
- the outcome of the DPIA

Step by Step Process to complete a Data Protection Impact Assessment

- 1) Project lead is commissioning service/ designing new project.
- 2) Project Lead completes the **Project Overview Form** and submits to the IG Hub for initial review. This form will identify if the new system/process will include the use of identifiable data (PID) by the ICB/CSU. A copy of the Project Overview Form can be obtained from mlcsu.ig@nhs.net
- 3) IG Hub compliance team carry out initial review and identify if the process requires a full DPIA or if a Data Protection assurance checklist is required.
 - a. **Full DPIA** required when the ICB is processing personal identifiable /pseudonymised data
 - b. **Data Protection assurance checklist** is required when the ICB is not processing personal identifiable /pseudonymised data but is the commissioning stakeholder and responsible for completing the due diligence on the project/service/appointed provider. A Data Protection Assurance Checklist can be obtained from mlcsu.ig@nhs.net
- 4) Compliance team pass to the IG Team Business Partner to arrange a meeting with the project lead to confirm if a full DPIA or Data Protection Assurance Checklist is to be completed.
- 5) IG Business Partner links in with the project lead to complete the legal, technical and security questions
- 6) IG Business Partner submits the DPIA/ Data Protection Assurance Checklist to DPO for review
- 7) DPO undertakes peer review against legislative requirements – seeks any required clarification or recommends for approval
- 8) If the process requires a Data Protection Assurance Checklist this is reviewed by SIRO for sign off. Governance checks are now complete and can be shared with Data controllers as part of their DPIA.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

- 9) If a full DPIA is required, the Caldicott Guardian reviews the DPIA considering the impact that this will have on data subjects and the risks to their data. Once the Caldicott is confident that all aspects have been covered they will recommend for SIRO approval.
- 10) Senior Information Risk Owner reviews the DPIA considering the risks to the organisation in processing or not processing the data for this purpose. Once all elements are completed satisfactorily the SIRO will undertake the final approval and approve pending the relevant agreements to be put in place and linked actions.
- 11) The IG Business Partner transfer the relevant information out of the DPIA into the relevant agreements – either Data Sharing Agreement, Data processor Agreement or Contract.
- 12) The IG Team to link in with the Data Controller to update the Privacy Notice to reflect the new or changed processing. Information Asset Registers and Dataflows should also be updated to reflect the new or changed processing.

Information Sharing

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The UK GDPR/DPA18 imposes a legal obligation on both parties to formalize their working relationship.

The ICB needs to ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits, failure to have in place an agreement is a breach of UK GDPR/DPA18.

This will provide the ICB with the assurance that both organisations understand their obligations, responsibilities and liabilities to help them comply with UK GDPR/DPA18.

The information sharing agreements document must include:

- the subject matter
- how long it is to be carried out for
- what processing is being done
- its purpose
- the type of personal data
- the categories of data subjects
- the obligations and rights of the data controller

For further advice and guidance on Information Sharing Agreements, please contact the Information Governance team.

30.0 Information Security Audits and Spot Checks

It is essential that all staff comply with the procedures put in place by the organisation to ensure information security. This helps minimise the potential risks to themselves and others, as well as reducing the financial costs arising from the loss of data, equipment and personal possessions.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

Potential security issues and risks should be identified and mitigated by implementing effective controls and solutions. The organisation’s main security objectives are:

- The protection of property against fraud, theft and malicious damage.
- The protection of all records and personal information, regardless of how these are held (electronic or paper records).
- The smooth and uninterrupted delivery of services.

In practice, this is applied through three cornerstones - Confidentiality, Integrity and Availability

- Information must be secured against unauthorised access – Confidentiality
- Information must be safeguarded against unauthorised modification – Integrity
- Information must be accessible to authorised users at times when they require it – Availability

All work areas within the organisation will be subject to Information Security audits and spot checks. The security measures of each building and office will be reviewed and their implementation will be tested. General working practices will be inspected through observations and interviews to ensure compliance with the security procedures and Information Governance guidelines.

The checks will consider:

- Physical security provisions of the building and offices
- Security applied to manual files e.g. storage in locked cabinets/locked rooms
- IT Security Processes e.g. screens locked when not in use
- Security of IT equipment and portable media when not in use
- Security of post handling areas
- Security of confidential fax handling
- Clear desk policy
- Clear screen policy
- Security of offsite storage boxes prior to removal to storage
- Evidence of secure waste disposal
- Use of whiteboards for confidential information

The spot checks will take place during the working day and early morning/late evening to provide a view of compliance both inside and outside of working hours. The focus of the checks may therefore vary dependent upon the time of the audit as some aspects, such as clear screen, may not be applicable outside of working hours.

In addition to the Information Security Spot Checks, audits will be carried out which, rather than being a general appraisal of compliance, will focus on specific information assets to verify and test the security measures specified as being in place in the asset’s entry in the Information Asset Register, including the methods of transmission for any associated data flows where possible (for example examination of emails to ensure they are encrypted would be beyond the scope of the audit). The audit would also consider arrangements for recording access to manual files where applicable, e.g. tracking cards, access requests under the UK GDPR/DPA18.

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

31.0 Useful Documents:

Contract, Temporary and Work Placement Staff Confidentiality and Compliance agreement

1. Confidentiality

- 1.1. In the course of your employment with Cheshire and Merseyside ICB (“the ICB”) you will receive and acquire confidential person/patient identifiable and commercially sensitive information that is the property of the ICB.
- 1.2. During and after your employment with the ICB you must take all reasonable steps to ensure the confidentiality of information that has been disclosed to or obtained by you is maintained.
- 1.3. You must not, either during or after your employment with the ICB:
 - Disclose any person identifiable or confidential information relating to the business or affairs of the ICB, its service users or associated entities unless specifically authorised to do so in writing.
 - Other than to the extent that is necessary to enable you to perform your duties:
 - make extracts from, copy or duplicate confidential information
 - make adaptations of confidential information
 - make use of confidential information for private purposes, or in any manner which may, or is calculated to cause injury or loss to the ICB, its service users, customers or associated entities; and
 - other than for the benefit of the ICB make notes, documents, working papers or memorandum relating to any matter within scope of the business of the ICB or concerning any of its dealings or affairs.
- 1.4. Clauses 1.2 and 1.3 shall continue to apply despite the termination or cessation of your employment by either the ICB or you.
- 1.5. Without limiting the generality of the above, for the purpose of this clause, “confidential information” means and includes any information relating to the ICB, its business and activity including but not limited to person and patient identifiable information and other sensitive information in whatever form but excluding any matter that has become public knowledge or part of the public domain and all other information provided to you which is either labelled or expressed to be confidential, or given to you in circumstances where one would expect the information to be confidential to the ICB.

2. Compliance

- 2.1. During your employment with the ICB it is a requirement that you comply with all relevant legislation. These shall include, but not be limited to:
 - a) UK General Data Protection Regulation/UK Data Protection Act 2018
 - b) The Human Rights Act 1998
 - c) The Crime and Disorder Act 1998

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final

d) Common Law Duty of Confidentiality

e) Freedom of Information Act 2000

2.2. In addition to the above-mentioned legislation, consideration may also need to be given to the following when sharing personal information:

a) The Caldicott Committee Reports

b) Information Security Standard ISO 27001

2.3. You will ensure that you understand the relevant elements of the applicable legislation that applies to your role within the organisation and ensure that you comply with legislation when carrying out your role.

2.4. During your employment with the ICB you will be required to comply with all relevant policies that are currently in place that relate to the sharing of information and confidentiality.

2.5. You will undertake mandatory Information Governance e-learning, and any other training as required, within the timescales specified by the ICB for any new starters within the organisation.

3. Deletion of data on Cessation

3.1. Upon cessation of your employment, you are required to deliver to the ICB all copies of information, including person identifiable information that you have used in the course of your official duties and to undertake that you will not use any person identifiable information for any use having terminated your employment with the ICB. You must also return any associated removable media in your possession.

I undertake to comply with the above obligations and conditions as required by the ICB and as stated above to protect the organisations confidential information and all relevant compliance requirements.

Name: _____
(Please print)

Signature: _____ Date: _____

Document Owner:	Approval date:	First published:
	Next review date:	Version: Final