

Our Ref: NG/RM/25321
Date: 1st October 2025

Nicola Griffiths
Deputy Director of Governance
North Staffordshire Combined Healthcare NHS Trust
Lawton House
Bellringer Road
Trentham
ST4 8HH

Reception: 0300 123 1535

Dear

Freedom of Information Act Request

I am writing in response to your e-mail of the 5th September 2025. Your request has been processed using the Trust's procedures for the disclosure of information under the Freedom of Information Act (2000).

Requested information:

I am writing to request information under freedom of information legislation, regarding your organisation's use of artificial intelligence (AI) technology/technologies.

I would be grateful if you could provide the following detail:

- 1) AI Systems in use
 - A list of tools, platforms or systems currently deployed or being piloted/trialled.
 - The purpose and function of each of the above.
 - **Microsoft Teams Premium – Intelligent Recap: Deployed to approximately 100 named users.**
Purpose: AI-generated meeting summaries, tasks and timelines to support productivity.
 - **Microsoft Copilot (Microsoft 365 Copilot / Copilot Chat): Limited pilot with approximately 5 named users.**
Purpose: Generative AI assistance for drafting, summarisation and reasoning over non-confidential content in Microsoft 365.
 - The departments or services where these are operational.
 - **Enabled on a named-user basis across corporate functions. No patient-facing clinical AI deployment.**
- 2) Procurement and development
 - Details of any contracts, tenders or partnerships with external providers for AI solutions. **No standalone AI vendor contracts beyond existing Microsoft 365 arrangements. Teams Premium and Copilot licences are procured as add-ons under existing Microsoft agreements.**

- Total expenditure on AI related technologies over the past three financial years, broken down by year.

3) Governance and Ethical Oversight

- Copies of, or information relating to, any internal policies, frameworks or guidance documents relating to the use of AI.

Please see Appendices 1-3 attached.

The Trust is in the process of developing AI policy.

- Any ethical review processes or risk assessments conducted prior to deployment.
DPIA process updated to include AI-specific questions, AI Security Assessment and AI & Data Protection Risk Toolkit.

- Details of any group responsible for the oversight of AI use within your organisation.
Managed through Information Governance (Head of IG & DPO), with SIRO/Caldicott oversight. AI Steering Group under redevelopment.

4) Impact on Workforce

- Any assessments, reports or internal communications regarding the impact of AI on staffing levels, job roles or workforce planning (including recruitment, redundancy).**No formal workforce impact assessment specific to AI.**

- Information on any roles that have been automated, restructured or made redundant due to AI implementation. **No roles automated, restructured or made redundant due to AI.**

- Details of any training, redeployment or upskilling initiatives offered to staff in response to the adoption of AI. **Training and guidance provided via AI User Guide and intranet resources.**

- Any consultations with trade unions or staff representatives regarding AI-related changes. **No AI-specific trade union consultations held to date.**

5) Performance and Evaluation

- Evaluations, audits or performance reviews of AI systems, as referenced in section 1. **No formal evaluations or audits yet for Teams Premium or Copilot.**

- Evidence of how AI systems have affected service delivery, decision-making or operational efficiency. **No evidence reports yet on service delivery or efficiency impact (pilot stage).**

6) Data protection and privacy

- Types of data used to train or operate AI systems, including whether this data is synthetic or not.

- **Teams Premium uses meeting artefacts (audio/transcripts) where enabled.**
 - **Copilot uses non-confidential Microsoft 365 content. No synthetic data created by the Trust.**
- Measures in place to ensure compliance with data protection legislation, including the DPA 2018 and UK GDPR.
 - **Mandatory DPIA for new AI tools.**
 - **Guidance covering lawful basis, transparency, bias awareness and human oversight.**
 - Procedures for handling bias, transparency and accountability in AI decision-making. **Guidance requires human verification of outputs and transparency (e.g., disclaimers).**

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review of the management of your request. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Dr Buki Adeyemo, Chief Executive, North Staffordshire Combined Healthcare Trust, Trust Headquarters, Lawton House, Bellringer Road, Trentham, ST4 8HH. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely



Nicola Griffiths
Deputy Director of Governance

Guidance on the Use of Artificial Intelligence (AI) Tools

Background

Artificial Intelligence (AI) refers to the development of systems that can perform tasks typically requiring human intelligence. This includes tasks like writing reports, making recommendations, processing data, problem-solving, language understanding, and decision-making.

The purpose of this guide is to support the safe, fair, ethical, and legally compliant use of AI tools, ensuring that data protection laws are upheld. AI is a rapidly evolving field, and this guidance will be updated as necessary to reflect changes in the technology.

Registering to Use AI Tools

You are permitted to register for popular AI tools, such as Google Gemini and ChatGPT, using your @combined work email address for **work purposes** only. However, you **MUST**:

- Use a password **different from** your work device login credentials.
- Adhere to all data protection and security policies as outlined below and in Trust Policies.

Acceptable Uses of AI Tools

Staff are allowed to use AI tools such as ChatGPT, Google Gemini, and Microsoft AI services for the following purposes:

- Composing non-confidential emails.
- Drafting reports or creating summaries of existing documents.
- Automating routine administrative tasks, such as generating meeting notes or formatting documents.
- Summarising non-confidential research or extracting key points from long articles.

Important Restrictions:

- **Do not input confidential data** into any AI tools. This includes patient information, staff personal details, and sensitive commercial data.

- The use of **Microsoft AI Tools** is allowed as long as they are not used to query or review patient or commercial data. You may use these tools to summarise non-confidential meeting transcripts, provided the outputs are checked for accuracy and include the disclaimer: *"These minutes were created through the use of AI."*
- **Microsoft Edge Co-Pilot** can be used to summarise web pages and articles but **MUST NOT** be used within browser-accessed clinical or care systems.

If you encounter a blocked or restricted AI tool, please contact the Information Governance (IG) team for advice on secure alternatives or obtaining necessary permissions.

Clinical Decision-Making and AI

AI tools can be useful in supporting clinical decision-making, but they should not replace your professional judgment. The final decisions about patient care must always be made in conjunction with the patient or service user, based on your clinical expertise.

AI outputs can assist with analysis, but you are responsible for ensuring that any AI-generated content aligns with clinical best practices and is thoroughly verified before being applied.

Risks and Responsibilities in Using AI

AI systems, particularly those operating on public networks like OpenAI's ChatGPT, **are not secure**. Data entered into these systems may be retained for training or used in responses to other users. Therefore:

- **Never input confidential or sensitive information** into AI tools. This includes patient records, staff personal data, financial details, or proprietary business information.
- **You are responsible for the accuracy** of AI-generated content. Always verify and cross-check AI outputs for factual correctness before using them.
- AI systems may introduce **bias** into their outputs. When reviewing AI-generated responses, consider the potential for bias, particularly regarding race, gender, or other sensitive characteristics, and ensure fairness in decision-making.

Failing to comply with these guidelines or exposing confidential data to AI platforms may result in disciplinary action and legal consequences under data protection laws.

- **Data Protection Impact Assessment (DPIA):** Before implementing any new AI tool or application, a **DPIA must be conducted** to assess the potential impact on individuals' privacy and identify any risks. Contact the Information Governance (IG) team for support in completing this assessment.
- **Legal Basis and Transparency:** Clearly communicate the **legal basis** for any data used in AI processing and maintain **transparency** with patients and staff. Inform them about how their data may be used by AI tools, especially if patient information is involved, even in a de-identified format.
- **Accuracy Documentation:** AI-generated outputs are **predictive, not factual**. All outputs used in decision-making must be documented and **verified for accuracy** by staff before being applied.
- **Data Minimisation and Alternatives:** Use only essential data in AI tools. Where possible, utilise **de-identified or synthetic data** rather than personal information to minimise risk, especially in research contexts.

Approval for Using AI Tools

Due to the rapidly evolving nature of AI, these guidelines cannot cover every possible use case. If you are uncertain whether a specific use of AI falls within this guidance, you must consult the Information Governance (IG) team at IG@combined.nhs.uk.

Before using an AI tool for purposes outside of this document's scope, obtain approval by providing a detailed case for review. The IG team will assess potential risks and ensure compliance with data protection laws and organisational policies.

Ethical Use of AI

When using AI tools, consider the following ethical guidelines:

- **Transparency:** If AI tools are used to generate documentation or emails, make it clear to your colleagues by informing them that AI was involved in the creation process.
- **Appropriateness:** Not all tasks are suitable for AI. Consider the context and ensure that AI is only used when it adds value without compromising human oversight.
- **Accuracy:** AI can sometimes produce incorrect, incomplete, or misleading information. Always double-check the content for factual accuracy, ensure clarity to prevent misunderstandings, and maintain the organisation's standards of professionalism.

Final Reminders:

- **AI is a tool, not a replacement for human judgment.** It should assist, not substitute, your expertise and discretion in both clinical and non-clinical tasks.
- Always **consider the limitations** of AI, including its potential for error, bias, and misunderstanding.
- **Never input patient, staff, or sensitive commercial information** into AI tools.

For any questions or concerns regarding AI use, please contact the Information Governance Team at IG@combined.nhs.uk.

Privacy Notice – Use of Artificial Intelligence

This privacy notice gives you information on how we protect your personal data when using Artificial Intelligence (AI) Tools. This includes software applications that incorporate AI technologies.

The National Cyber Security Centre has defined AI as: *'Any computer system that can perform tasks usually requiring human intelligence. This could include visual perception, text generation, speech recognition or translation between languages'*.

Our contact details

Name: North Staffordshire Combined Healthcare NHS Trust
Address: Lawton House, Bellringer Road, Trentham Stoke-on-Trent ST4 8HH
General phone number: 0300 123 1535
Website: www.combined.nhs.uk

We are the controller for your data. A controller decides on why and how data is used and shared.

Data Protection Officer contact details

Our Data Protection Officer is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at DPO@combined.nhs.uk.

Our Use of AI Tools

The use of AI is the biggest and fastest moving change to computing in recent years. It is a new technology that requires careful governance to ensure its use is safe and does not expose personal data about our service users and staff to unnecessary risk. Examples of its use include:

- Generation of business meeting notes and any action points
- Generation of summaries of multi-disciplinary team meetings where our service users and patients cases are discussed

Governance of AI

We are aware of the risks when using AI. It is totally dependent upon development and training so, we must be mindful of some key risks:

- It can get things wrong and present incorrect statements as facts (a flaw known as 'AI hallucination')
- It can be biased and is often gullible when responding to leading questions
- It can be coaxed into creating toxic content as it is prone to 'prompt injection attacks'
- It can be corrupted by manipulating the data used to train the model (a technique known as 'data poisoning')

Before their use is approved, AI Tools are subject to enhanced Data Protection Impact Assessments for the specific use case requested. These are considered by the Deputy Chief Digital Information Officer to decide if they are fit for use.

We see AI as a tool to support our work. However, ownership and accountability will always remain with our staff members who use and double check the product generated by AI, eg the accuracy of a clinical note.



Chair: Janet Dawson
Chief Executive: Dr Buki Adeyemo
www.combined.nhs.uk

Follow us on Twitter/X: @CombinedNHS
Follow us on Facebook: www.facebook.com/NorthStaffsCombined



We are a diverse and inclusive Trust and there is no place in our organisation for discrimination, harassment or personal abuse

We have internal policies and training in place to ensure that our staff adhere to the highest standards of confidentiality.

Only authorised personnel will have access to confidential information.

Lawful Basis

The lawful basis to process your personal data does not change because we use AI: This notice is in addition to our standard Privacy Notices which can be viewed on our website: [Privacy and GDPR - North Staffordshire Combined Healthcare Trust](#)

Which AI Tools will we use?

We are starting to use Generative Artificial Intelligence (GenAI) such as Microsoft Co-Pilot and ChatGPT. These AI Tools can be standalone products or can be embedded into other services. They give us the ability to create human-like text and context and answer questions in a conversational manner.

They are used to simplify processes to improve the efficiency, quality and speed of our business processes so valuable clinical staff time can be better used in delivering patient care. As time progresses, we will expand the use of AI but each use case will be subject to the same high level of scrutiny.

For further information contact:

Data Protection Officer

North Staffordshire Combined Healthcare
NHS Trust

Lawton House

Bellringer Road

Trentham

Stoke-on-Trent ST4 8HH

Email: DPO@combined.nhs.uk

Information Commissioner

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

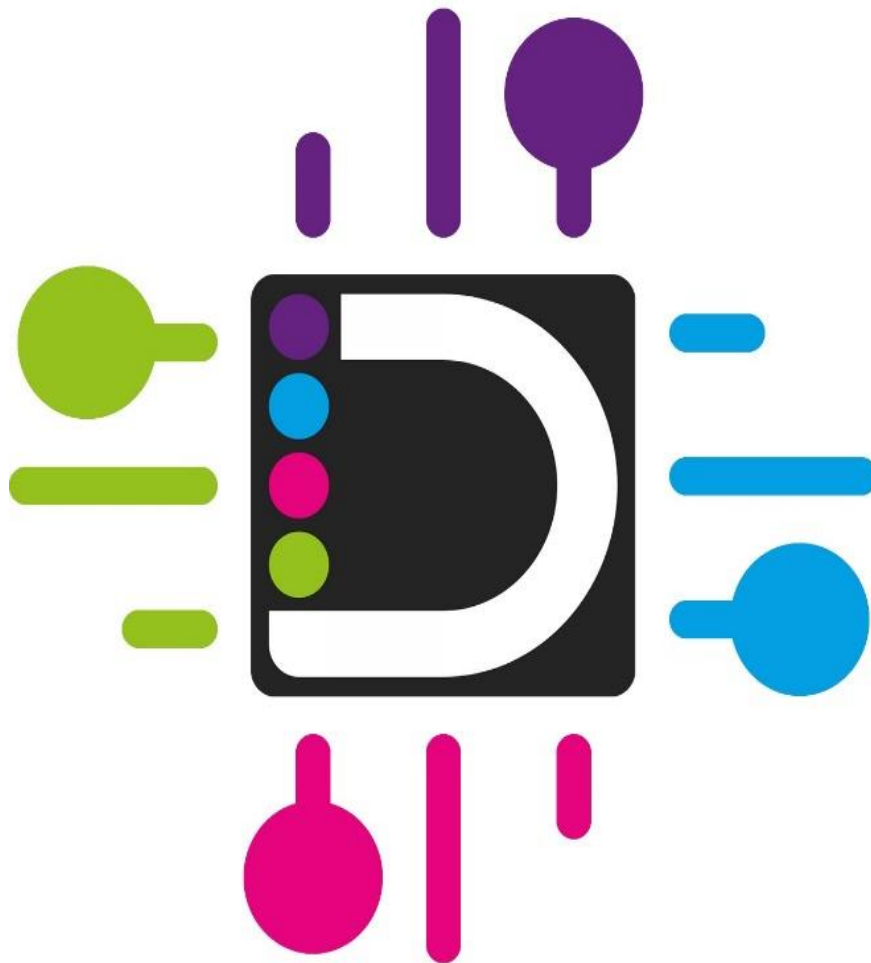
Cheshire SK9 5AF

Telephone: 01625 545745

<https://ico.org.uk/>

North Staffordshire Combined Healthcare NHS Trust Information Governance Handbook

Information Governance Your data, secured



Contents

Glossary of Terms.....	6
General IG Do and Do Not's.....	10
1. Introduction	11
2. Legislation and Regulations.....	11
3. Principles of the Data Protection Act 2018	12
4. Data Protection Officer	13
5. Caldicott Principles	13
6. Confidentiality	13
7. Summary of key roles and responsibilities.....	14
8. Premises Security.....	14
8.1 ID Badges	14
8.2 Access Control	15
8.3 CCTV.....	15
9. Clear Screen and Clear Desk	16
9.1 Clear Screen.....	16
9.2 Clear Desk	16
10. Information Governance Induction for New Starters.....	17
11. Annual Data Protection Training.....	17
12. Individuals Rights	17
13.1 Timescales to respond to a SAR	20
13.2 Fees.....	20
13.3 Failures to meet requests for information	20
13.4 Who should requests be directed to?	20
13.5 Responding to requests for personal information from the Police	20
14. Freedom of Information	21
14.1 What information is covered by the Act?	22
14.2 What are the Trust's obligations under the Act?	22
14.3 Processing a FOI request	22
15. Information and Data Security	23
15.1 Registration Authority/Smartcards.....	23
15.2 Line Manager responsibilities	23
15.3 Staff Smartcard Code of Practice	23
15.4 Abuse of Privilege	23
15.5 Data Security.....	24

15.6	Remote working and portable devices	24
15.7	Remote working and portable devices best practice guidance	25
15.8	Trust Mobile Phones	26
15.9	Use of Personal Mobiles	27
15.10	Passwords and PIN codes	28
15.11	Role-Based Access	28
15.12	Third Party Access to Network.....	29
15.13	Prevention of Misuse	29
15.14	Improper Access and Disclosure of Records	29
15.15	Software Licensing Procedure	30
15.16	Unauthorised Installation of Software	30
15.17	Individual Responsibilities	30
15.18	Disposal of Equipment and Reuse of Surplus Equipment	31
16.	Internet and Intranet.....	31
16.1	Permissible Access	31
16.2	Non-Permissible Access.....	31
16.3	Monitoring.....	32
16.4	Unintentional Breaches of Security	32
17.	Acceptable Use of Social Media and Social Networks	32
17.1	Personal use of social media at the workplace and at home	32
17.2	Using social media for professional purposes	33
17.3	Setting up a unique social media presence for specific service/campaign	33
17.4	Interacting with existing external social media sites	33
17.5	Considerations when using Social Media	34
17.6	Approval Process for access to Social Media.....	34
17.7	General usage guidance	34
18.	Safe-Haven Procedures – Sending Person Confidential Data or Commercially Sensitive Data	35
18.1	Safe-Haven Email Procedures.....	35
18.2	Trust Email Encryption Facility	35
18.3	Safe-Haven Post Procedures.....	36
18.4	Internal Post Procedures	36
18.5	External Post Procedures	37
18.6	Safe-Haven Telephone Procedures.....	37
18.7	Safe-Haven Room Requirements	38
18.8	Safe-Haven Room Procedures	38

19. Email	39
19.1 Email Retention	39
19.2 Dos and Don'ts of Email	39
19.3 Sending emails to mailing/distribution lists	40
19.4 Recalling emails	40
19.5 Monitoring.....	40
19.6 Shared Email Access.....	41
20. Text Messaging	42
20.1 Text Messaging to communicate with patients	42
20.2 Text Messaging Consent	42
20.3 Text Messaging Dos and Don'ts	43
21. Video and Teleconferencing	43
21.1 Responsibilities.....	43
22. Microsoft Teams	44
22.1 Etiquette when using Teams	44
22.3 Staff Guidance when using Teams	45
22.4 Meetings/Calls when using Teams.....	46
23. Data Security and Protection Incidents	47
23.1 What is a data breach?	47
23.2 What are the types of breaches?	47
23.3 When is an incident reportable under DPA18/UK GDPR?	47
23.4 Steps staff should take following a Data Protection Breach/Cyber Security Incident	49
24. Records Management	50
24.1 Identification/Naming of Records	50
24.2 Naming of electronic records.....	50
24.3 Naming Conventions.....	51
24.4 Naming of paper records	51
24.5 Version Control.....	51
24.6 Classification	52
24.7 Electronic records storage.....	52
24.8 Paper records storage	53
24.9 Usage/Transfer of Records.....	53
24.10 Retention and Disposal of Records.....	56
24.11 Retention Periods	56
24.12 Disposal.....	57

25. Business Continuity Plans	57
26. Information Risk Assessment and Management Programme.....	57
26.1 Managing Information Assets.....	58
26.2 Person Identifiable Data Flow Mapping.....	58
27. Data Protection Impact Assessment (DPIA)	59
28. Information Sharing	59
28.1 Sharing Information for Direct Care Purposes	59
28.2 Sharing Information for Indirect Care Purposes.....	62
29. Information Security Audits.....	62
30. Consultation and Ratification Schedule	63

Glossary of Terms

Term & Acronym		Definition
Anonymisation	Anon	It is the process of removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous
Artificial Intelligence	AI	Any computer system that can perform tasks usually requiring human intelligence. This could include visual perception, text generation, speech recognition or translation between languages
Breach Management Process	BMP	Process of managing any breach of personal information, providing guidance on what to do when a breach is identified including investigation, root cause analysis and lessons learned
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
The Care Computer Emergency Response Team	CareCERT	Delivered by NHS Digital to provide proactive advice and guidance about digital threats and cyber security best practice. Includes CareCERT Knowledge, CareCERT Assure and CareCERT React
Code of Conduct		A set of rules to hold staff accountable to the highest standards for the way they handle, process and share personal information
Common Law Duty of Confidentiality	CLDC	When someone shares personal information in confidence, it must not be disclosed without some form of legal authority or justification
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 finds 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 information

Data Processor	DP	A natural or legal person, public authority, agency or other body which processes personal information on behalf of the controller
Data Protection Act 2018 (DPA18)	DPA18	Legal framework to protect personal information about living individuals
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with UKGDPR requirements. A mandatory requirement and must be undertaken whenever handling, process or sharing personal information
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation
Data Security and Protection Toolkit	DSPT	<p>A mandatory, annual online self-assessment tool managed by NHS Digital to demonstrate compliance with the National Data Guardian Review's 10 data security standards.</p> <p>With effect from September 2024, the National Data Guardian standards are being replaced by the National Cyber Security Centre's Cyber Assessment Framework (CAF) as the new basis for DSPT assurance.</p>
Data Sharing and Processing Agreement	DSPA	Sets out the purpose of the data sharing and processing, covers what happens at each stage, sets standards and helps all parties involved in the sharing and processing to be clear about their roles and responsibilities
Data Subject	DS	Any living individual whose personal information is collected, held or processed by an organisation
Direct Care	-	<p>A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering on individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual. It includes:</p> <ul style="list-style-type: none"> • Supporting individuals' ability to function and improve their participation in life and society • The local audit/assurance of the quality of care provided • The management of untoward or adverse incidents • The measure of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care <p>Does not include research, teaching, financial audit, service management activity or risk stratification</p>

Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities
Hardware Assets	HA	The equipment used to house systems, store information etc and includes desktop computers, laptops, mobile phones, tablets and USB memory sticks
Human Rights Act 1998	HRA98	Legislation that lets you defend your rights in the UK courts and compels public organisations to treat everyone equally, with fairness, dignity and respect
Indirect Care	-	Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine and medical research.
Information Assets		Assets that contain information, for example databases, audit data, policies and procedures, records and reports, contracts and agreements and business continuity plans.
Information Asset Administrator	IAA	Providing support to the IAO, the IAA is the individual who uses the information asset on a day-to-day basis. Often works in an administrative capacity
Information Asset Owner	IAO	Senior/responsible individual whose role it is to understand the information their teams hold, any additions/removals to assets, who has access to information and to support on updates to the Trust's Information Asset Register
Information Commissioner's Office	ICO	The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals
Information Governance	IG	How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently and effectively and in a manner which maintains public trust
Information Risk Programme	IRP	Programme of identifying the Trust's assets, how they are stored, who has access to them, how they are communicated and then risk assessed so appropriate security measures can be applied to protect the information

Legitimate Relationship	-	The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care
Personal Information	PI	Any information that relates to an identified or identifiable individual. which is related to an identified or identified natural person. What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or cookie identifier or other factors
Privacy and Electronic Communications Regulations 2003	PECR	Sits alongside the DPA18 and UKGDPR giving people specific privacy rights in relation to electronic communications
Pseudonymisation	Pseud	Replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified
Public Interest Test	-	This applies with the holder of the information believes that the public good that would be served by sharing the information outweighs both the obligation of confidentiality owed to the individual and the public good of protecting trust in a confidential service
Record Lifecycle	RL	Records lifecycle in records management refers to the stages of a records 'life span': from its creation to its preservation (in an archive) or disposal
Records Management Code of Practice 2021	RMCoP21	Guidance produced to support NHS organisations in keeping records, including how long to keep different types of records. Replaces all previous versions
Senior Information Risk Owner	SIRO	Board member who is familiar with information risks and the Trust's response to risk. The role of the SIRO is to take ownership of the Trust's information risk policy, act as an advocate for information risk on the Board and provide written advice to the Accounting Officer on the content of their annual governance statement in regard to information risk
Subject Access Request	SAR	A written request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act
System Assets	SA	Assets that relate to the systems the Trust uses for example, email systems, network drives, software both externally bought or developed in-house
UK General Data Protection Regulation	UK GDPR	The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UKGDPR' sits alongside an amended version of the DPA18

General IG Do and Do Not's

Do	
Familiarise yourself with IG policies and the contents of this handbook	✓
Seek advice and guidance if you are unsure at any time with regards confidentiality, privacy or security of personal information	✓
Report anything suspicious	✓
Safeguard the confidentiality of all personal information	✓
Clear your desk of personal information at the end of the day	✓
Lock your computer screen if you leave your desk for any length of time (ctrl, alt, delete and enter or Windows key and L	✓
Ensure that you cannot be overheard when discussing confidential matters	✓
Share only the minimum information necessary	✓
Transfer personal information securely when necessary	✓
Use email 'cc' or 'bcc' with care	✓
Report any actual or suspected breaches of confidentiality or loss of information or data. Use the Trust incident reporting process or via your line manager	✓
Maintain your annual IG training	✓
Ensure personal information is disposed of correctly	✓
When dealing with a data sharing and processing agreement, please consult the IG team (IG@combined.nhs.uk)	✓
Do Not	
Do not share login or passwords or leave them lying around for others to see	✗
Do not share personal information unless there are statutory grounds to do so	✗
Do not use personal information unless absolutely necessary	✗
Do not collect, hold or process more information than you need and do not keep it for longer than necessary	✗
Do not discuss personal information in public	✗
Do not download from doubtful sources	✗
Do not use illegal software	✗
Do not leave personal information lying around	✗
Do not plug USB such as data or memory sticks or other devices without permission from S&SHIS SMT: Log in	✗
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 the S&SHIS helpdesk and ask them to open it SMT: Log in	✗
Do not have whiteboards with personal or corporate information in view by general public	✗
Do not agree to any data sharing and processing agreements without the DPO agreement	✗

[Return to contents page](#)

1. Introduction

This handbook is intended to provide information to support and assist NSCHT 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 - [Policies - CAT](#).

Information Governance (IG) is the practice used by all organisations to ensure that information 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

We hold large amounts of personal, personal confidential and sensitive information. All staff should be able to provide assurances that Information Governance standards are incorporated within their working practices.

Personal and sensitive information can be contained within a variety of documents, held both electronically and manually; for example:

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

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

These will include, but not be limited to:

- Team retention period 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. 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:

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

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. Principles of the Data Protection Act 2018

When processing data, the following principles must apply and must be embedded into everyday activities across the Trust:

Principle 1 Personal information shall be processed lawfully, fairly and in a transparent manner	Principle 2 Collected for a specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes	Principle 3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Principle 4 Accurate and where necessary, kept up to date	Principle 5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed	Principle 6 Processed in a manner that ensure appropriate security of the personal information including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

4. Data Protection Officer

Under DPA18/UK GDPR the appointment of a Data Protection Officer (DPO) became mandatory. It is especially important for health organisations who process personal and sensitive information on a daily basis.

5. Caldicott 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	Description
1	Justify the purpose(s) for using personal information
2	Don't use personal information unless absolutely necessary
3	Use the minimum necessary personal information
4	Access to personal information should be restricted to required or relevant staff
5	Everyone with access to personal information should be aware of their responsibilities
6	Understand and comply with the law
7	The duty to share information for individual care is as important as the duty to protect patient confidentiality
8	Inform patients and service users about how their personal information is used

6. Confidentiality

We all have the responsibility to use personal information 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 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 information about any living individual who can be identified from that information or from other information which in the possession of or is likely to come into the possession of the data controller (example, the Trust).

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, removable media and tapes.

It also includes personnel records including those held by line managers, as well as those held centrally by personnel departments.

The use of all such personal information is controlled by the Data Protection Act principles above.

[Return to contents page](#)

7. Summary of key roles and responsibilities

Role	Responsibilities
Senior Information Risk Owner	Executive Board member with allocated lead responsibility for the Trust's information risks and provides the focus for management of information risk at Board level. NSCHT's SIRO is Elizabeth Mellor, Chief Strategy Officer.
Caldicott Guardian	The person with overall responsibility for protecting the confidentiality of personal information and for ensuring it is shared appropriately and in a secure manner and acts very much as the conscience of the patients/service users putting their best interests at the heart of any decision making. NSCHT's Caldicott Guardian is Dennis Okolo, Chief Medical Officer.
Data Protection Officer (DPO)	Role mandated by the Data Protection Act 2018. The DPO acts in an advisory capacity advising what can and cannot be undertaken within the realms of the legislation.
Information Governance Team	<p>The Information Governance Team is responsible for providing support to NSCHT in a wide range of areas including:</p> <ul style="list-style-type: none">• The annual submission of the data security and protection toolkit requirements• Support and guidance on investigating data protection and cyber incidents• Offering advice and ensuring the Trust complies with legislation, policies, and protocols• Developing IG training materials and raising awareness• Processing subject access requests, both patient and staff requests• Supporting with the completion of mandatory Data Protection Impact Assessments• Developing Data Processing/Sharing Agreements when required• Supporting the Trust's Information Risk Programme, ensuring all assets are accurately recorded and regularly reviewed• Undertaking Data Protection Audits to ensure staff demonstrate compliance with key data protection principles

8. Premises Security

8.1 ID Badges

All staff should wear their ID badge always whilst on any Trust site or when representing the Trust in an official capacity. ID badges are personal to the user and should not be passed to unauthorised personnel or loaned to other members of staff.

The loss of an ID badge should be reported immediately to your Line Manager and to the Information Governance Team and an incident logged accordingly, although please note that this would not be an IG breach as it is not a breach of data protection or confidentiality.

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

8.2 Access Control

It is essential that access is tightly controlled across all Trust sites. Where possible all access to work areas should be restricted.

Visitors to any Trust site should be asked to report to reception where they will be asked to sign the visitor's 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

All 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 NSCHT's expectations regarding use of identity badges.

8.3 CCTV

We use CCTV across some of its sites to provide safety to staff and patients alike. The sites with CCTV installed are:


- Ashcombe Centre
- Bennett Centre
- Darwin Centre
- Dragon Square
- Greenfield Centre/Summers View
- Harplands
- Lawton House
- Lymebrook Centre
- Sutherland Centre

We comply with the requirements of the ICO Code of Practice when using CCTV around its sites, and also aligns with the following legislation:

- Freedom of Information Act
- Protection of Freedoms Act
- Human Rights Act
- Surveillance Camera Code of Practice

9. Clear Screen and Clear Desk

9.1 Clear Screen

- Laptops, PCs, and mobile devices should be locked when they are not in use regardless of how long they will be left unattended (i.e., to go to the toilet or to speak to a colleague at their desk, etc.). For Windows operated 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 5 minutes idle 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 leaving site at the end of each shift or when closing down your equipment when working remotely from home/other site. This enables any security and system updates to be rolled out and installed when the device is restarted
- When working on site in an office or in a clinical area, 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

9.2 Clear Desk

- 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. This applies when working remotely from home or another site
- Staff who are required to attend meetings or leave their desks unoccupied for any amount of time should remove any confidential information from their desks
- 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 NSCHT confidential information such as salaries and contracts
- Staff should also be aware that information left on desks is more likely to be damaged or destroyed in a disaster such as fire, flood, etc
- Any visitor, appointment or message books should be stored in a locked area when they are not in use

[Return to contents page](#)

10. Information Governance Induction for New Starters

It is vitally important that all new staff are made aware of the Trust's Information Governance requirements at the earliest opportunity and clear guidance is given about their own individual responsibilities for compliance. Particular emphasis must be placed on how IG requirements affect day-to-day working.

11. Annual Data Protection Training

All staff are required to complete mandatory annual data security awareness (IG) training. The training is available via the Learning Management System (LMS) and Managers will ensure staff remain compliant with this training at all times.

12. Individuals Rights

Right	Details
The Right to be Informed	<p>Trust Privacy Notices are available primarily through the Privacy Pages on the Public Facing Website</p> <p>The purpose of the privacy notices is to inform the public about the collection and use of their personal information. All staff need to be aware of these notices and be able to direct individuals both to the notices and where they can contact if they have any queries or concerns, usually the data protection officer.</p> <p>Changes to existing privacy notices or identifying the need for new privacy notices are captured by the data protection impact assessment process.</p>
The Right of Access	<p>Individuals including staff, have the right to ask the Trust for confirmation of whether they process information about them and if the Trust does, to have access to that information, so the individual is aware and can verify the lawfulness of the processing.</p> <p>This is called a Subject Access Request.</p>
The Right to Rectification	<p>If personal information that the Trust holds is found to be inaccurate or incomplete, individuals have the right to have it rectified.</p> <p>The individual can make a request for rectification either verbally or in writing and the Trust has one calendar month to respond to such requests. All such requests should be sent to the IG team in the first instance.</p> <p>The right to rectification is not an absolute right. Requests deemed to be unfounded, excessive or repetitive in nature or the record in question must be maintained as evidence, can be refused.</p> <p>Each request is considered and acted upon on a case-by-case basis.</p>
The Right to Erasure	<p>Individuals have the right to have personal information that the Trust holds about them erased and to prevent processing in specific circumstances:</p>

	<ul style="list-style-type: none"> • Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed • If the individual withdraws their consent for the Trust to process their information (if this was the basis on which it was collected) • The personal information was unlawfully processed • The personal information has to be erased in order to comply with a legal obligation <p>However, if the Trust collected and is processing information about an individual to comply with a legal obligation for the performance of a public task or because the processing is necessary for the provision of health or social care or the management of health or social care systems or services, then the right of erasure does not apply.</p> <p>The individual can make a request for rectification either verbally or in writing and the Trust has one calendar month to respond to such requests. All such requests should be sent to the IG team in the first instance.</p> <p>Each request is considered and acted upon on a case-by-case basis.</p>
The Right to Restrict Processing	<p>Individuals have the right to ‘block’ or suppress the processing of their personal information. If this right is exercised, the Trust can still store their information but not further process it and will retain just enough information about the individual to ensure that the restriction is respected in future.</p> <p>Subject to the following:</p> <ul style="list-style-type: none"> • Accuracy of the information that the Trust holds is contested, the Trust will restrict the processing until the accuracy of the data has been verified • Trust is processing the personal data for the purposes of a public task • If the processing of the personal information is found to be unlawful but they oppose erasure and request restriction instead • The Trust no longer needs the data held about the individual, but the individual requires the data to establish, exercise or defend a legal claim <p>Potential methods of restriction include:</p> <ul style="list-style-type: none"> • Temporarily moving the information to another processing system • Making the information unavailable to users • Temporarily removing published data from a website

	<p>Requests for restriction can be made both verbally or in writing and the Trust has one calendar month to respond to such requests. All such requests should be sent to the IG team in the first instance.</p> <p>Each request is considered and acted upon on a case-by-case basis.</p>
The Right to Data Portability	<p>This right allows the individual to obtain and reuse personal information they have provided to the Trust for their own purposes across different services. It allows them to move, copy or transfer personal information easily from one IT environment to another in a safe and secure way, without hindrance to usability.</p> <p>Only applies if consent or performance of a contract are the Trust's lawful basis for processing the information.</p> <p>Requests for data portability can be made both verbally or in writing and the Trust has one calendar month to respond to such requests. All such requests should be sent to the IG team in the first instance.</p> <p>Each request is considered and acted upon on a case-by-case basis.</p>
The Right to Object	<p>Individual as the right to object to the Trust processing their information. They must have an objection on grounds relating to their particular situation.</p> <p>If an objection is raised, the Trust will no longer process the information unless it can demonstrate compelling legitimate grounds for processing which can override the individuals interests, rights and freedoms or the processing is for the establishment, exercise or defence of legal claims.</p> <p>Objections can be made both verbally or in writing and the Trust has one calendar month to respond to such requests. All such requests should be sent to the IG team in the first instance.</p> <p>Each request is considered and acted upon on a case-by-case basis.</p>
Rights in relation to automated decision-making and profiling	<p>Automated individual decision-making is a decision made by automated means without any human involvement.</p> <p>As the Trust does not make any decisions based solely on automated processing, this right does not apply.</p>

13. Access to Information- Subject Access Requests

Every living person, or an authorised person acting on their behalf, 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 and all staff need to be aware of Subject Access Requests, how to identify a valid request and who to direct such requests to.

Requests can be made verbally or in writing and does not need to specify it is a Subject Access Request nor does a request need to mention the Data Protection Act 2018 to be valid. Identity is required to validate any request along with proof of authority to act in the case of third-party requests. Records held by Trust can be in manual (paper records) or digital form and may include such documentation as clinical records, hand- written notes, letters, reports, imaging records, photographs, DVD, and sound recordings.

[Return to contents page](#)

To note – Anything documented on a corporate means of communication (work email, MS Teams, instant messages, e.g., WhatsApp on a work mobile) is eligible for release under a subject access request, so please be mindful of what you write in emails and messages, as it could find itself being released as part of request.

13.1 Timescales to respond to a SAR

Under DPA18/UK GDPR information requested must be provided without delay and within **one month**. In certain circumstances, an extension to this timeframe can be applied, allowing for a further 2 months to process the data. If applying an extension, the requestor must be informed of this and informed of when they would be expected to receive their information.

13.2 Fees

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

13.3 Failures to meet requests for information

Failure to comply and provide information requested under DPA18/ UK GDPR could result in a substantial fine. Individuals also retain the right to pursue a claim in court.

13.4 Who should requests be directed to?

All requests should be made via the Trust Subject Access Portal: [Combined SAR Portal](#)

The portal is used to receive requests for personal information as well as securely issue the information to the requester.

13.5 Responding to requests for personal information from the Police

If the police contact the Trust requesting personal information on patients or staff, this will need to be dealt with based on the seriousness of the case and appropriate police authority level and be vigilant at all of times of phishing requests in comparison with genuine requests.

Cyber criminals will often mimic official organisations to try and extract information so take the required steps to ensure the request is a valid one. There may be times when it is appropriate to challenge a request from the police.

Remember the following:

- The police need to provide sufficient information to describe the seriousness of the case (justification for the request). You should not feel under pressure to provide personal information and never give the police any original paperwork to take away
- Authority levels – applications should be authorised by a substantive Chief Inspector or Superintendent
- Where possible the request should be made via the SARs portal: [Combined SAR Portal](#)
- If requests are received via email, the subject heading should describe, in summary, the contents of request email (e.g. proof of life enquiry– missing from Stoke-on-Trent since April 2017) should be used – the Police follow the guidance as provided by the National Crime Agency so this should also help to formalise a request
- Any member of staff may be asked for information in the event of an emergency, out of hours request or in occurrences where the usual Manager/Team Lead is unavailable

- Request for any relevant information must be passed to a specified contact in the police force and include Police Officer's name, address, telephone number, email address and Police ID number
- Applications need to demonstrate proportionality, legality, accountability, necessity and justification for any information
- We should only share the necessary and proportionate information
- The Trust's Caldicott Guardian will be involved in authorising the release of information to the police if it falls outside of normal IG procedures

In setting out why it would be lawful for a NHS organisation like NSCHT to provide information with the police under the UK GDPR and DPA 2018 in relation to a missing person, the Trust would be able to provide information in relation to a missing person to the police. Under Article 6(1) of the UK GDPR, which sets out the lawful processing bases. The Trust can lawfully provide information in relation to a missing person to the police on the basis of: ***(d) processing is necessary in order to protect the vital interests of the data subject, and (e) processing is necessary for the performance of a task carried out in the public interest.***

The common law duty of confidentiality will be satisfied when information is shared:

- Where there is a clear statutory obligation to share confidential information
- With the consent of the individual concerned
- Where it is in the best interests of an individual who lacks the capacity to consent to the sharing
- Where the public interest served by sharing the minimum information needed to satisfy a purpose outweighs both the duty of confidentiality owed to an individual and the public interest in services being seen to be provided on a confidential basis

You should satisfy yourself that any disclosure is required by law and, if necessary, ask the police what legal basis are they relying on or what act are they making the application under. E.g. prevention, detection of crime.

Document in the record the information disclosed, who authorised the disclosure, to whom, when and on what basis; and whether the data subject was informed or not.

In addition, there are a number of legal gateways that enable sharing of information, for example:

- **Court orders** - These include Police and Criminal Evidence Act, 1994 applications and applications in respect of coroners' investigations (Coroners and Justice Act 2009)
- **Safeguarding** - Information must be shared for child or vulnerable adult safeguarding purposes (for example, under s.47 Children Act 1989)

[Return to contents page](#)

14. Freedom of Information

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.

14.1 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, and 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 have to 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

14.2 What are the Trust's obligations under the Act?

Making information available is only valuable to the public if they know they can access it, and what is available. The Trust 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 Trust
- Provide contact details for making a request, including a named contact and phone number for any enquiries about the Act
- The Trust 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 Trust services

14.3 Processing a FOI request

A request for information under the Freedom of Information Act 2000 must:

- Be received in writing – verbal Freedom of Information requests cannot be accepted
- Email requests and requests via a social media platform are acceptable. Requesters do not have to mention the Act or direct their request to a designated member of staff
- State the name of the requester and an address/email address for correspondence
- Clearly describe the information requested
- Be responded to within 20 working days

[Return to contents page](#)

15. 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.

15.1 Registration Authority/Smartcards

Smartcards are required to use and access IT systems essential to healthcare provision. Individuals are granted access to a Smartcard by the Trust Digital Team, whose job is to verify the identity of all healthcare staff who need to have access to patient identifiable or sensitive data. 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.

15.2 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 refer 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 Digital Team, of any leavers, starters, and staff changes

15.3 Staff Smartcard Code of Practice

- Use your Smartcard responsibly and in line with your access rights
- Inform the Digital 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. In particular 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, provide suitable identification, and attend 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 Trust's suite of IG policies and procedures; adhere to the UK GDPR and Caldicott Principles, and the Confidentiality Code of Practice and the Care Records Guarantee

15.4 Abuse of Privilege

It is strictly forbidden for employees to look at any information relating to their own, family, friends, work colleagues or acquaintances records. In cases where a close friend, partner or spouse or relative is, or becomes, a patient or service user, it is the responsibility of the employee to inform their line manager that such a relationship exists.

The line manager will discuss the situation with the employee and agree an appropriate course of action. It may be appropriate for the patient or service user to be treated by another clinician or team, or in the case of an inpatient admission, for the employee to be moved to another area for the duration of the patients or service users treatment.

Employees must also not access the patients or service users records, as this will be classified as a non-authorised access to clinical records and will be considered a breach of Trust policy, which could result in dismissal.

Staff must not abuse their position by viewing any information regarding ‘VIP or celebrities’, unless they are directly involved in their care.

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

15.5 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.

Information, whether in paper or electronic form, is of high importance to NSCHT, therefore the Trust 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 section). 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, and all relevant equipment in compliance with Trust leaver’s process. If a leaver is moving to another NHS Trust, Pharmacy, GP Practice etc. smartcards will remain with the leaver and be reactivated upon appointment at the new employer. Only if an employer is leaving the NHS completely will they need to surrender their Smartcard upon leaving
- 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 because of their actions. The organisation will investigate all suspected and actual security breaches.

15.6 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 and portable devices.

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 the Information Governance Team.

15.7 Remote working and portable devices best practice guidance

- Encryption is mandatory in all mobile devices used to store identifiable data
- 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
- 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 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
- All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information
- 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 Trust 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 Manager/IG Team
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available
- Sensitive corporate and Personal Confidential Information must not be stored or transferred using any unencrypted “USB Memory” device
- 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 and the IG Team
- Staff must ensure that the mobile devices are used appropriately at all times
- Staff should not under any circumstances use any mobile device whilst in control of a vehicle
- Ensure that other ‘non’-authorised users are not given access to the device or the data it contains

[**Return to contents page**](#)

15.8 Trust Mobile Phones

Any staff member who has been issued with a mobile phone or uses a SIM card provided by the Trust must ensure they adhere to strict codes of practice in relation to its use. The Trust has a Safe Use of Mobile Phones Policy and a Mobile Device Policy, which all staff with a Trust-issued mobile must read and ensure they follow the guidance on using the phone appropriately. This guidance applies to the use of phones in both clinical and non-clinical areas.

Mobile phones play a significant role in people's lives and are an essential item of equipment for staff; their uses are numerous and include:

- Communicate in a variety of ways, including voice, text, email and video including virtual consultation with patients
- Provide information from an application or web browser
- Take, store and share photographs and videos
- Vehicle navigation
- Provide supplementary safety for lone workers

The Staffordshire and Shropshire Health Informatics Service (SSHIS) who provide the Trust's IT support services are responsible for ensuring that policies and procedures are followed in relation to mobile phones. Duties of the team include and are not limited to:

- The secure storage of phones and SIM cards
- Working with the purchasing team to recommend new phones
- Setting up of new phones, including installing Mobile Device Management software and updating both the Trust and service provider databases
- Reassigning used phones and SIM cards
- Ensuring that the users sign and accept the conditions of use for phones and SIM cards
- Where a user changes departments, arrange for the service provider to change the cost code on their database
- On a monthly basis, obtain the list of staff who have left the Trust from HR, check the supplier database and where applicable suspend/cancel any SIM cards
- Recall all phones which are non-compliant

During periods of absence, which includes sickness absence and maternity leave, managers should discuss and agree with staff whether a mobile phone will be required. Where a phone is not required, it should be returned by hand to the SSHIS who will suspend the SIM card and either hold or re-use the phone. It remains staff responsibility to understand the workings of the phone and how to use it properly.

All staff using a Trust-assigned mobile phone or SIM card must ensure they adhere to the confidentiality requirements as contained in the Trust key data protection policies. Phones must be used in a reasonable, appropriate and lawful manner and wherever possible, must connect to the Trust or private Wi-Fi to reduce costs and also to obtain permission from a manager if required to make premium rate or international calls.

Staff members must ensure they take reasonable steps to prevent damage, theft or loss of a device and report any such incident to their Line Manager and the Information Governance

Team as soon as possible. Any misuse of a Trust-assigned mobile phone or SIM card will be handled by the Trust's disciplinary policies. Any staff member leaving the Trust must return their Trust mobile phone or SIM card to their Line Manager as part of their exit arrangements.

15.9 Use of Personal Mobiles

Bring Your Own Device (BYOD) is now available for **corporate staff that do not work with clinical data**.

To improve security, personal mobiles must be enrolled which allows the Trust to mandate certain security features such as ensuring that a pin is set on the device and that encryption is enabled. This also allows the Trust to remove information from the mobile when staff no longer work for the Trust.

Enrolling your device will allow you to use Apps to access your work email, OneDrive, Teams etc on your personal device. If you do not wish to enrol your device, you must use your work device to access Trust information.

We reserve the right to:

- Deny access to work O365 systems if your personal device is running versions of software and operating systems that are not secure
- Remotely wipe Trust information from your personal device if it poses a risk to the organisation or its information

The Trust and S&SHIS cannot see your personal information when you enrol your device. We only have the ability to manage the applications and accounts that are installed for the Trust – we will not be monitoring your activity.

What we can see	What we can't see
Device Owner and Device Name	Calling and web browsing history
Device Serial Number	Email and text messages
Device Model	Contacts
Device Manufacturer	Calendar
Operating System and Version	Passwords
Device IMEI	Pictures including what's in the photo app or camera roll
App inventory and app names for managed work apps	Files

The Trust remains in control of the information for which it is responsible, regardless of the ownership of the device used to carry out the processing.

BYOD User Responsibilities

- Familiarise yourself with your device and its security features so you can ensure the safety of Trust information
- Invoke relevant security features
- Ensure that your device is not used for any purpose that would be at odds with our IT and IG policies
- Ensure that your device is not used for illegal activities
- Ensure that accounts are logged out of when not in use

- Ensure that no other person accesses Trust information
- Prevent theft and loss of data and report any loss to S&SHIS as soon as you become aware so that the device can be wiped of Trust information
- Keep Trust information confidential where appropriate
- Take responsibility for any software you download onto your device
- Ensure that personal devices do not hold any information that is sensitive, personal, confidential or of commercial value
- Not use any device that has had its terms of service broke, such as a 'jailbroken' device

[Return to contents page](#)

15.10 Passwords and PIN codes

In line with the National Cyber Security Centre best practice, bear the following in mind when setting your passwords:

- Minimum password length is 14 characters (try three random words that you will remember such as 'tyrecabbagedog' but not any versions of 'password')
- There is no need for capital letters, special characters, number etc in your password
- You can't re-use the last 20 passwords
- Passwords expire annually, every 365 days
- Don't re-use the same password across important accounts. If one of your passwords is stolen, you don't want the criminal to also get access to, for example, your banking account
- 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
- Store your passwords in your browser when prompted; it's quick, convenient and safer than re-using the same password. Browsers can also detect 'dodgy' websites that phishing emails try and trick you into visiting
- The Trust has set up 2 Factor Authentication (2FA) when setting up accounts. It's called 2FA because it involves signing into your account using two passwords or codes; one that you know, and the other usually sent to your phone. Even if a criminal knows your passwords, they will struggle to access any accounts that you've protected by turning on 2FA

15.11 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
- 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 DPA18/UK GDPR

- Access should be requested via your Line Manager/IG Team

15.12 Third Party Access to Network

Third parties will not be given access to Trust systems or networks unless they have formal authorisation to do so.

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, e-Referral Services etc. they are required to provide IG assurances via the Data Security and Protection Toolkit (DSPT) as part of business/service support processes or contractual terms, which is 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, e-Referral Services 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 Trust's Breach Management Process and an investigation will take place to decide the outcome.

[Return to contents page](#)

15.13 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

15.14 Improper Access and Disclosure of Records

Health and care records can include a wide range of material including:

- Electronic records
- Handwritten notes
- Correspondence between health professionals
- Visual and audio recordings
- Communications with patients (including text messages, emails)
- Test results/X-rays/Photographic Images

It's fair to say that many improper disclosures of patient information are unintentional but can cause significant harm, upset or distress. You must be careful not to use data in an inappropriate way, which includes:

- If having conversations in reception areas, at a patient's bedside and in public places be very careful as you could easily be overheard
- Ensuring notes and records cannot be seen by other patients, unauthorised staff, or the public and are managed securely at all times.
- Patient details can be lost if handover lists are misplaced, or when patient notes are in transit so always be vigilant and careful when handling patient information
- Any personal information about patients that you hold or control is effectively protected at all times against improper access, disclosure or loss
- Not leaving patients' records, or other notes you make about patients, either on paper or on screen, unattended
- Not sharing passwords under any circumstances – we have to ensure all system access is audited and as such every staff member must user individual log-ins
- **Not accessing a patient's personal information unless you have a legitimate reason to view it; never look at records out of curiosity as it not only a disciplinary offence but individuals can be prosecuted for accessing an individual's records without a legitimate need to do so**
- Not share personal information about patients under any circumstances – disclosing personal information about a patient is a very serious matter

15.15 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 Digital Team. Contravention of the recommendations may be considered a disciplinary offence.

15.16 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 Trust networks and/or file servers. To intentionally introduce files which cause damage to computers may result in prosecution under the Computer Misuse Act 1990.

15.17 Individual Responsibilities

Individuals must not install software onto a Trust provided desktop, laptop, or another mobile device. Doing so constitutes a disciplinary offence.

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

Should you suspect the presence of unauthorised software on your system you should report it to the S&SHIS, 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, the Digital Team and the IT Service provider.

15.18 Disposal of Equipment and Reuse of Surplus Equipment

Should it not be possible to reuse equipment internally within NSCHT, 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 provider.

This is to ensure that the Trust:

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

16. Internet and 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 the NSCHT's policy on acceptable use. NSCHT 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.

[**Return to contents page**](#)

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 libelous, blasphemous, or defamatory. This list is not exhaustive. Other than instances which demand criminal prosecution, NSCHT 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 the IT Service provider who may liaise with the Information Governance Team to determine whether access can be granted or not.

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 S&SHIS and the IG Team.

17. Acceptable Use of Social Media and Social Networks

The content below is intended to give you general guidance only – refer to the Trust Social Media Policy.

NHS organisations are 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 communication 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 a number of 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, including temporary workers, bank/agency staff working or assigned to NSCHT 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 Trust 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 handbook provides guidance on the use of social media tools by NSCHT employees in a personal capacity. For example, this includes a personal profile on Facebook, Twitter, and Instagram etc. in a personal capacity by NSCHT employees.

It is important to remember that adherence to the expectations set out in this handbook applies equally whilst at work or when out of work, when any inference is made to work, either specifically or indirectly.

Staff or contractors/temporary/bank/agency workers working for or assigned to NSCHT must be aware of their association with NSCHT when using social media. If they identify themselves as an employee of NSCHT, they should ensure that their profile and any related content is 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 a NSCHT 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 NSCHT. For example, employees should not write or report on conversations, meetings or matters that are meant to be private or internal to the Trust.

Unauthorised disclosure of confidential information would constitute misconduct/gross misconduct in accordance with NSCHT's 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 NSCHT 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.

17.3 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)

[**Return to contents page**](#)

17.4 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

17.5 Considerations when using Social Media

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

- 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 Trust
- Disclaimers on social media sites do not remove NSCHT’s obligations to accuracy and implications
- Comments made to a social network site belonging to NSCHT can be disclosed under the Freedom of Information Act 2000
- When NSCHT creates an account on a social networking site such as Twitter or Facebook, the Information Commissioner has dictated that the Trust must be able 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 start to process accordingly

17.6 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 a Trust employee they MUST follow the following procedure:

- Obtain approval from Line Manager/IG Team
- For communications on behalf of the Trust or a partnership of which the Trust is a member, a business case should be made which will be considered and referred to directors with recommendations
- 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/IG Team before proceeding. Managers unsure of which sites, forums or tools are acceptable for use should speak to the IG Team

17.7 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/temporary/agency/bank staff working for or assigned to the Trust should 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.

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 behaviour. They must take care to avoid online content or actions that are inaccurate, libelous, defamatory, harassment, threatening or may 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.

[Return to contents page](#)

18. 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 across the Trust to ensure personal information or commercially sensitive information is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the Trust whether this is by post or other means.

If such information needs to be sent inside or outside of the organisation by post, 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 personal or commercially sensitive information, it should be considered whether it would be sufficient to send anonymised or pseudonymised information instead.

18.1 Safe-Haven Email Procedures

When sending emails containing personal or commercially sensitive information, the email **must** be sent from your Trust NHS email address to ensure the highest level of security.

18.2 Trust Email Encryption Facility

Any emails that contain personal or commercially sensitive information must be encrypted before they are sent – it is easy to do – just type [SECURE] at the beginning of the subject line.

If you are pressured to send without encryption, please contact the IG Team (IG@combined.nhs.uk)

If an external organisation tells you that they are unable to open/access encrypted emails that we send to them, here is the process they need to follow:

1. When an encrypted message is received, click the button to read the message
2. A browser window will open offering several ways to access the encrypted message. The easiest way is to 'Sign in with a one-time passcode'. This will send a message with the code to recipient
3. When the code is received it will be valid for 15 minutes
4. Enter the passcode and click continue
5. The encrypted message will now be displayed
6. Email recipient can reply to messages within the window and the reply will be encrypted

If they are still unable to open the email once these steps have been followed, they need to contact their IT department and ask them to allow the message through – we are unable to help them with this issue.

Always double check email addresses are correct before pressing 'send'.

If you are sending an email to multiple recipients, always use 'BCC' so that their individual email addresses cannot be seen by the other recipients.

[Return to contents page](#)

18.3 Safe-Haven Post Procedures

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

- **Never** use internal envelopes or previously used envelopes, instead use tamper-proof envelopes – it is the responsibility of teams across NSCHT to ensure they are appropriately stocked with tamper-proof envelopes in various sizes
- 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
- Where the information is being sent to
- Initials of the person responsible for sending the information
- Request that the recipient confirms receipt

18.4 Internal Post Procedures

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

Secure Green Bags

- 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 and includes a return address
- Place into the internal mail ready for sending
- Request that the recipient confirms receipt

If you do not have a Secure Green Transport Bag, please contact the Information Governance Team (IG@combined.nhs.uk) who will supply one.

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

[Return to contents page](#)

18.5 External Post Procedures

When sending personal 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.

18.6 Safe-Haven Telephone Procedures

When sharing personal 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:

- 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 Line Manager or Information Governance Team

- If speaking to a patient, 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 cannot overhear other confidential conversations that may be going on in the background
- Ensure that you cannot be overheard when providing personal information
- Ensure that you do not leave any person identifiable information on answer machines/voicemail

18.7 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/patients
- 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 and in view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use

18.8 Safe-Haven Room Procedures

- A list of staff authorised to enter a Safe Haven room must be maintained. Those staff listed will need to be authorised by the Trust Caldicott Guardian
- Only staff named on the 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
- 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 be kept locked at all times, even when the room is in use
- No personal 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

[Return to contents page](#)

19. 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.

[Records Management Code of Practice - NHS Transformation Directorate](#)

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.

19.2 Dos and Don'ts of Email

Users may not use the NHS / NSCHT 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 libelous messages
- To breach the DPA18/UK GDPR
- To forward chain/junk email

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

- Ensure that all emails that contain personal information or commercially sensitive information are encrypted before they are sent
- Write well-structured e-mails
- Use short, descriptive subjects
- Signatures must adhere to NSCHT standards – a template email signature is available on the Trust intranet site
- 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 particular 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 absolutely necessary
- Email should be treated like any other correspondence and should be answered as quickly as possible
- When on annual leave or away from work for any reason, the Out of Office facility should be used and clear Automatic Replies set ensuring the message is set for both internal messages and those from external organisations
- 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 DPA18/UK GDPR
- 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

19.3 Sending emails to mailing/distribution lists

If an email is to be sent to several 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 which allows the email addresses of the other recipients to be concealed.

This means that the recipient list of the email cannot be re-used, and it reduces the chances that the recipients will receive spam or viruses because 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.

[Return to contents page](#)

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 similar as the recall function will not work.

19.5 Monitoring

The Trust ensures 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 Trust's disciplinary policy.

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

The Trust allows Managers within their professional capacity to 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, staff 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 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 RICA, should there be a necessity for an employee to use their work email for personal emails, it is recommended that they put the word '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 Trust network, it becomes the responsibility of the Trust to protect it under the DPA18/UK GDPR.

[Return to contents page](#)

19.6 Shared Email Access

There may be circumstances where there is a work requirement to regularly access another staff members emails 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 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.

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.

20. Text Messaging

All clinical, patient, corporate and other information shall be managed in accordance with the NHS Confidentiality Code of Practice.

The Trust owns all content sent using the Trust's facilities and all information stored on its servers or cloud facilities.

20.1 Text Messaging to communicate with patients

Text (SMS) messages are used primarily for appointment confirmation or reminders. However, services in the Trust may use electronic messaging for other purposes which must be approved by the IG Team and included in local procedures, or, if a one-off exercise, by documenting the intended use and having it authorised by the service manager.

The uses made of text messaging and the service rules governing the contents of messages will vary from one service to another depending upon the nature and sensitivity of the particular service.

20.2 Text Messaging Consent

- Where relevant, it should be made clear to patients that text messaging will not be monitored and therefore will not be responded to, outside normal working hours
- Prior to sending electronic messages to any patient, informed consent must be obtained by explaining all the appropriate information to them
- Consent must be obtained and recorded in the specific place for consent recording in the patient's record in the Trust's clinical system
- Patients must be made aware that they can opt out of the service at any time in the future
- When asking to use consent for text messaging, patients must be made aware of their responsibility to keep the services they use up to date with their correct number or email address that they wish to be contacted on
- Patients should be made aware of all options for communication (phone, letter, text, email) and their preferences recorded on the Trust's clinical system
- It should be made clear to the recipient that any correspondence will be added to their record

[**Return to contents page**](#)

20.3 Text Messaging Dos and Don'ts

Record all communications by electronic messaging and transcribe them into the patient's health record including the date and time sent or received and the phone number or email address it was sent to or from	✓
Make patients aware that text messages must not, under any circumstances, be used in emergency situations and should be advised of the correct method(s) of contacting in an emergency	✓
Ensure texts are written in full without using 'text speak' or abbreviations	✓
Keep text messages formal and maintain professional standards. Avoid giving personal comments	✓
Ask the patient to clarify any abbreviations or 'text speak' they have used in an electronic message, make no assumptions	✓
Always respond to messages within an agreed timescale where relevant	✓
Only send text messages within normal working hours	✓
Only use a Trust issued mobile phone for sending text messages to patients, no other phone should be used	✓
Once an incoming text message has been transcribed and entered into the patient's records, it should be immediately deleted from the phone account	✓
In case a text message is seen by someone other than the intended recipient, avoid using unnecessary identifiers of the patient or service	✓
Text messages should only be sent from the Trust issued mobile of the appropriate staff member of the approved system for sending texts. Text messages must only be sent to the phone number provided by the patient or carer to which they have consented to the Trust using; no other phone numbers should be used	✓
Do not use inappropriate language in text messages that could cause offence, such as swearing or racial comments. If you receive any such message, it should be reported via the Trust online Incident Reporting System and fully detailed with a verbatim transcription in the patient's record	✗
Do not use predictive text as this can cause unintended modification and change or confuse the meaning of the message	✗
Do not use electronic messages to convey personal or sensitive information	✗

[Return to contents page](#)

21. Video and Teleconferencing

21.1 Responsibilities

Video and teleconferencing have become powerful ways for organisations to communicate and collaborate but can be open to abuse 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.

The use of such equipment will also contribute to the Trust's ability to communicate with patients and health providers especially.

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:

- All participants must identify themselves at the beginning of the consultation and when speaking, to ensure patients are aware who they are talking with
- No participants shall be expected to invite others to take part in the meeting or session without the express consent of the chair
- Headsets should be worn for all meetings or sessions where participants can be overheard by others and webcams should be used where they cannot be overseen by others outside the invited participants
- Where a participant enters or 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 or leaving with their name and job role
- 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

Chair of the meeting or session

The chair is responsible for the overall running of the meeting or 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 or 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 or 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.

Meeting/Session Participants

All participants are expected to adhere to this guidance. No additional recordings are to be made without the express permission of the chair before the meeting or session commences.

Participants are encouraged to wear headsets to ensure that other staff may not overhear the conversations unless in a private room where the device audio can be utilised, and any webcams used should not be overseen by others where possible.

22. Microsoft Teams

22.1 Etiquette when using Teams




As a result of the COVID-19 pandemic, and the need for people to work remotely from homes, NSCHT rolled out Microsoft Teams to all staff. This meant that staff could work effectively using

the latest technology to chat, call, video, and engage at any time, bringing everybody closer. Documents, photographs, videos, chat history and meeting notes are available at all times, making it far easier to work together. MS Teams enables teams to set up their own space with all the apps that are needed, enabling a more connected and collaborative approach to remote working. There are however, a number of safety considerations when using MS Teams:

- All staff using MS Teams must do so in line with The Trust's Acceptable Use Policy
- Security of MS Teams is an integral part of the Trust's system security responsibilities, and when access to information is required, it is important that confidentiality and integrity of the information is upheld, and adequate protections are in place in line with both the Trust's policies and procedures but also in line with statutory requirements
- Team owners must ensure that Teams created for Trust purposes should be deleted by the owner when the related project or programme has been completed
- Inactive Teams will be automatically deleted after 6 months of inactivity and **completely unrecoverable** from the recycle bin after another 30 days following their deletion
- Documents shared via MS Teams that need to be kept after the project has ended must be saved in the relevant shared folder on the Trust's servers. Documents must be held according to the Trust's record retention periods as detailed in the NHS Records Management Code of Practice 2021
- All Teams created by staff should use a name that clearly identifies the use or purpose of the Team and must not include anything inappropriate, offensive or hateful words, or any 'code' words that represent these things
- MS Team sites are provided to include members from across the organisation and external organisations. When creating Teams for use with external organisations, the group must be marked as Public

22.3 Staff Guidance when using Teams

- **Be transparent** - Use your own name and photograph within your Office 365 profile. It is important that members are clear about who they are interacting with
- **Be safe** - MS Teams is designed to support secure networks, therefore, do not over disclose personal information and protect yourself against identity theft
- **Safeguard data you share** – If it is not advocated that we use MS Teams to share personal identifiable information, but if personal identifiable information is to be shared in a Team, the Team owner is responsible for managing the members of that Team and ensuring the appropriate safeguards are in place
- **Only post to appropriate members** - All MS Team channels and discussions are visible to all members of the MS Team site. Private messaging is available to send direct messages to selected members
- **Be professional** - Be polite and treat team members with respect. It is important that this is maintained throughout and even in instances when opinions differ. Be clear and avoid using ambiguous language which may be open to misinterpretation
- **Keep it relevant** - Make sure you clearly understand the purpose of your MS Teams site. Stay on topic and avoid sharing irrelevant content as this may frustrate other members

- **Safeguard all data** - MS Teams provides a file storage location for files posted within conversations and channels. This provides a time limited repository and should not be used as a substitute for personal storage such as One Drive, staff personal drives or departmental files storage. The Trust and Microsoft cannot guarantee data previously saved to this location can be restored after the site is closed
- **Be aware** - When sharing images and videos - ensure that the sharing of images and videos does not breach image rights and copyrights. Seek permission from anyone included in personal photographs prior to sharing them
- **Sharing information** - Do not share information outside of your private teams - information shared within your private Team is for use by the Team members only and should not be shared outside without appropriate permission. No confidential, personal or sensitive information should be shared outside of your private teams
- **Only create new MS Teams when you must** - Make sure there is not a Team already created that meets your requirements
- **Don't over-invite people to your MS Teams** - Make sure you have the right people in your MS Team and remove people should they leave the Trust to ensure accuracy is maintained
- **Make your out-of-office response MS Team-friendly** - Your Outlook out-of-office response displays in MS Teams as well. Instead of saying "Thank you for your email" rephrase to "Thank you for your message"
- **Reactions are meant for sentiment** - The **thumbs-up** is good for acknowledging messages which can help keep work on task. Please be careful when using other emoji's as they can be misinterpreted. If you are going to use emoji's like **love, laugh, wow, sad** and **anger**, then please only use in private messages and not in public channels
- **Use private chat for high-priority questions or to chat to colleagues** - use private chat the way you would any other instant messaging service
- **Pay attention to your colleague's availability status** - You will be able to see the status of your colleagues, for example:
Available  Away  Busy / Do not disturb 
- **Do not assume you have privacy** - Chats can be audited by the IT administrators. Do not say anything in chat that you would not say to someone in person and be mindful that chats can form part of any Subject Access Requests processed by the Trust
- **Adding participants to a private chat** - When adding a participant to a private chat, this allows them to see prior discussions in the chat. Before adding anyone into an existing private chat, be sure about whether you want them to see what has been previously discussed

[Return to contents page](#)

22.4 Meetings/Calls when using Teams

- **Join promptly** – ideally join a few minutes before the start of the meeting to ensure the meeting can start at the scheduled time
- **Microphones** – keep your microphone on mute when not talking to reduce background noise in the meeting

- **Backgrounds** – only blur the background if you want to hide your own background. If choosing an image for your background the preference would be the Trust Corporate background ([Templates - CAT](#)), and not pictures of beaches, superheroes or other animated images
- **Use the chat function** – if you are in large meetings especially the chat function is useful to share thoughts and comments or use the “hands up” emoji to let the chair know you have a point to raise
- **Recording meetings**- if you have the functionality to record a meeting, please ensure you have obtained the consent of all members
- **Headphones** – use headphones if you are not in a private area for the meeting

23. Data Security and Protection Incidents

It is important that information remains safe, secure, and confidential at all times. All staff are encouraged to follow NSCHT’s Incident Reporting process, using the Ulysses system to present an auditable record of the incident as soon as possible following the identification of the incident.

In addition to the internal reporting of incidents, it is a legal obligation under DPA18/UK GDPR to notify serious personal data breaches to the ICO within 72 hours.

ONLY THE DATA PROTECTION OFFICER CAN REPORT INCIDENTS.

All health and social care organisations are to use the reporting tool accessed via the Data Security and Protection Toolkit to report data breaches.

23.1 What is a data breach?

A **data breach**, as defined under DPA18/UK GDPR, 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’)

23.2 What are the types of breaches?

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

23.3 When is an incident reportable under DPA18/UK GDPR?

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 again. The incident must be graded according to the impact on the individual or groups of individuals and not the Trust.

The **significance** is further graded rating the incident on 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).

Grade the potential **significance** of the adverse effect on individuals using the guide below:

No	Effect	Description
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 the 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

No	Effect	Description
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

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

There are a limited number of circumstances where even when the Trust 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 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 can 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.

[Return to contents page](#)

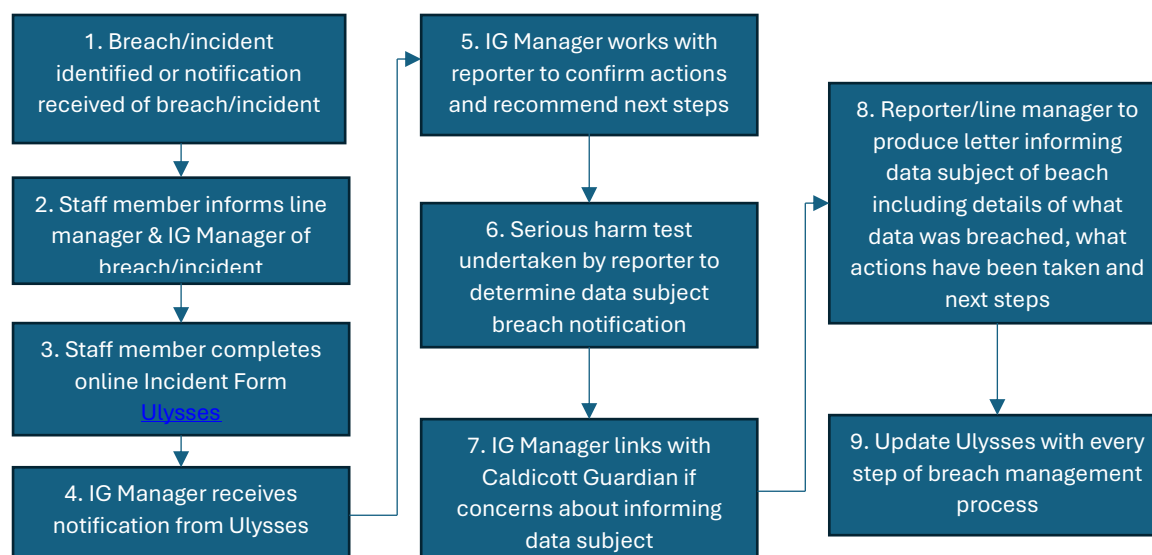
Breach Assessment Grid

Anything other than ‘grey breaches’ are reportable. Incidents where the grading result is in the red are required to be reported within 24 hours.

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

23.4 Steps staff should take following a Data Protection Breach/Cyber Security Incident

It is important that staff understand the role they play if a breach/incident has occurred or they have been made aware of a breach. Incidents need to be reported in a methodical way allowing the Trust the opportunity to adhere to strict breach management protocols. The following steps should be undertaken:



24. Records Management

Records Management is the process by which the Trust 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 NSCHT 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 DPA18/UK GDPR to fulfil Subject Access Requests.

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.

24.1 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.

24.2 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:

- **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

[Return to contents page](#)

24.3 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., JOHN SMITH or JOHN'S 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\2021-22\2021-10-11 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\2021-2022 rather than Audits\ Audits 2021-2022\)
- 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)

24.4 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)

24.5 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 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.

24.6 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 sub-categories 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 accessible to the public under legislation such as the Freedom of Information Act 2000.

24.7 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 etc.).

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.

NSCHT advocates using 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.

[Return to contents page](#)

24.8 Paper records storage

Good quality documentation standards are essential to provide accurate records of the Trust'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 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.

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.

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.

24.9 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.

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 so 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:

- Effective aides to identify documents and records, provide 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. There is a Trust tracer system within Lorenzo and the historical data system on the staff intranet

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 relocation

It is a business need that from time to time, teams may be required to 'relocate' from one premise to another. It is during these times that the Trust 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 NSCHT records. This procedure relates to the movement of **ALL** 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

The Trust have a Decommissioning Policy that covers any work carried out by moving contractors, whilst under contract with NSCHT. This also includes the expectations and responsibilities placed upon staff, working for the contracted companies, who will be moving the records.

[Return to contents page](#)

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 Trust and the contractors undertaking the relocation of the records to ensure the secure removal of records.

The responsibility for ensuring the security of records during moves lies with the individual teams within the Trust and not the Information Governance 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

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
- 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 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.

[Return to contents page](#)

24.10 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 DPA18/UK GDPR. If the Trust continues to hold information which they do not have a need to keep, they would be liable to disclose it upon request. The DPA18/UK GDPR also advises that we should not retain personal data longer than is necessary.

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

24.11 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:

[Records Management Code of Practice - NHS Transformation Directorate](#)

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:

<http://www.england.nhs.uk/ourwork/tsd/ig/ig-resources/>

24.12 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.

25. Business Continuity Plans

Business Continuity Planning is a method used to identify potential impacts that may threaten the operations of the Trust.

The fundamental element of business continuity is to ensure that whatever impacts the Trust, that it continues to operate and with minimal disruption to patients, service users and staff.

Business continuity plans will help shape the Trust's 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).

The Trust has 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.

26. 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 at all times protected, available and accurate to support the operation and continued success of the organisation.

A number of key activities in the Data Security and Protection 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

[Return to contents page](#)

26.1 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	training materials
data files	operational/support procedures
contracts and agreements	business continuity plans
system documentation	back up plans
research information	audit trails
user manuals	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
annual leave sheets
sickness absence returns
expenses
papers for meetings

Examples of electronic assets include:

spreadsheets
annual leave/sickness records
local databases
scanned documents
electronic copies of letters

26.2 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 included in confidentiality audits forming part of the compliance requirements of the Data Security and Protection 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 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 Trust 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 and relevant legislation (DPA18/UK GDPR) 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. Fines of up to £17,500,000 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 DPA18/UK GDPR.

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 any part of the Trust. This information is then risk assessed to identify areas of high risk and any areas of non-compliance with the Trust's safe-haven procedures.

Through this process, the Trust will actively identify and review where person confidential information is held, processed, or shared to ensure a legal basis for doing so is identified. Where no legal basis can be found an Information Governance 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. A new electronic information asset register will be in use from Q2 2025 and staff will be trained accordingly.

27. Data Protection Impact Assessment (DPIA)

The Trust has produced some guidance around DPIAs – see link below:

[!\[\]\(7510f031844ad4008a55bb76ecaf4be0_img.jpg\) Data Protection Impact Assessments \(DPIAs\): What You Need to Know](#)

Our DPIA template is based on the NHS England Universal DPIA template.

[Return to contents page](#)

28. 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 DPA18/UK GDPR imposes a legal obligation on parties to formalise their working relationship through information Sharing and Processing Agreements. Our DPIAs form the basis of our information sharing and processing agreements that are based on the NHS England Universal DSPA template.

The Trust has ensured that appropriate mechanisms are in place to enable reliable and secure exchange of data within the legal limits as failure to have such mechanisms in place constitutes a breach of DPA18/UK GDPR.

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

The information sharing agreements document must include:

- the subject matter
- how long the sharing of information 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

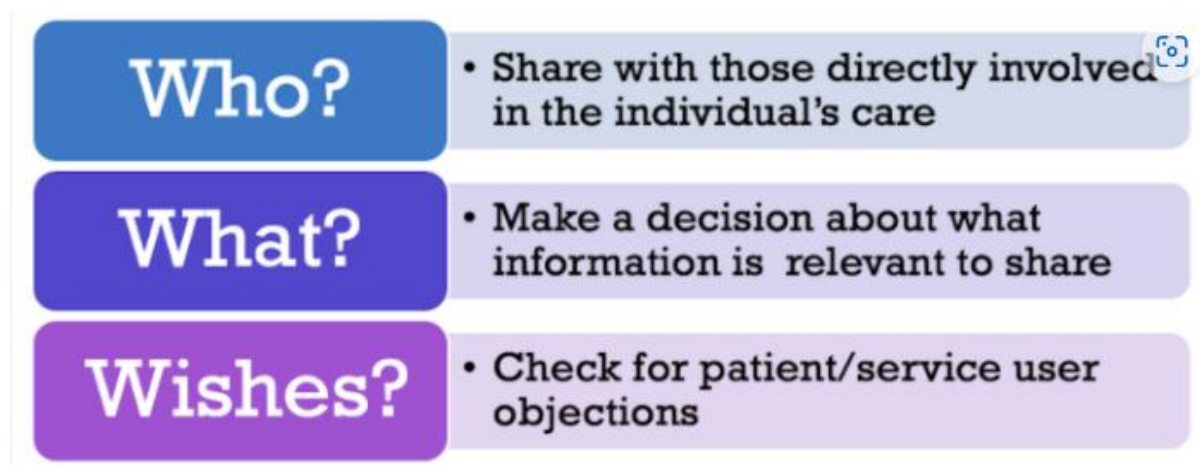
28.1 Sharing Information for Direct Care Purposes

Health and social care professionals have a legal duty to share information to support direct care. The law and the Caldicott Principles support staff to share relevant information in order to provide care and support to a patient or service user.

The duty to share information for direct care is as important as the duty to protect confidentiality.

When sharing patient information, there are a number of points which should be considered so that information is shared appropriately:

- **Legitimate and appropriate purpose**
 - We have a legal basis to share information for direct care: UKGDPR Article 6 (1) (e) – Public Task and UKGDPR Article 9 (2)(h) – health and social care purposes
- **Verify the external provider's role**
 - Ensure the provider is a legitimate health and social care entity involved in the patient's care
- **Apply the minimum necessary rule**
 - Only share the information required for the external provider to deliver care
 - Avoid sharing excessive or irrelevant information
- **Use secure methods of communication**
 - Email: Use encrypted email
 - Phone calls: verify the recipient's identity before discussing patient details
- **Document the information sharing**
 - Record what information is being shared by way of a data sharing and processing agreement – contact the IG Team (IG@combined.nhs.uk).



Sharing information for direct care purposes scenarios (non-IG staff)

1. Nurse-to-Nurse handover between wards

A staff nurse on Ward 1 calls a nurse on Ward 3 to hand over a patient who is being transferred. They discuss the patient's current condition, test results, treatment plan and any safeguarding concerns.

Role involved: Registered Nurse

Purpose: Continuity and safety of care

Legal Basis: Direct Care under UKGDPR Article 6(1)(e) – Public Task and Article 9(2)(h) – Provision of health or social care

2. Social Worker collaborating with Mental Health Services

A social worker supporting an NHS mental health patient shares safeguarding and risk information with the CMHT for ongoing case planning.

Role involved: Social Worker (working within or alongside NHS)

Purpose: Coordinated care

Legal Basis: Direct Care/safeguarding – covered under UKGDPR

The staff in these scenarios do not need IG team involvement for routine, lawful direct care information sharing.

Sharing Information for direct care purposes that require IG approval scenarios

1. New information being shared between organisations without an existing agreement

The Trust plans to start sharing patient information with a new provider that doesn't yet have a data sharing and processing agreement (DSPA) in place.

Why is IG needed?

A DSPA must be established and approved by the Data Protection Officer (DPO) and Caldicott Guardian to ensure legal, secure sharing and that responsibilities are documented.

2. Large-Scale data extraction for direct care planning

A clinical system admin or member of performance wants to extract a full patient list with diagnoses and medications to support direct care planning for a new service line.

Why is IG needed?

Bulk data sharing – even for care – requires a Data Protection Impact Assessment (DPIA) and assurance around how data is used, stored and accessed.

3. Use of new digital tools or third-party apps for direct care

A clinical team wants to start using a new third-party app to manage video consultations.

Why is IG needed?

IG staff must assess data security, hosting, contracts and ensure compliance with standards and best practice.

28.2 Sharing Information for Indirect Care Purposes

The term 'indirect care' is defined as activities that form part of the provision of services to the population or a group of patients with a particular condition, but which fall outside of the scope of direct care.

This includes health services management, preventative medicine and medical research.

You cannot imply consent for the use of confidential information for purposes outside of direct care.

It is generally accepted that consent can be implied for activity concerned with the quality of assurance of care, but only when the audit is undertaken by those who are part of the direct care team.

Examples of indirect care purposes

1. Research and Statistics
 - Using anonymised or pseudonymised patient data to study trends or outcomes
 - Clinical trials and health studies
2. Service Planning and Commissioning
 - Using patient data to assess demand for services and allocating resources
 - Informing policy or healthcare planning decisions
3. Audit and Evaluation
 - Ensuring quality and safety standards are being met
 - Reviewing clinical performance
4. Regulatory and Legal Obligations
 - Reporting to the CQC
 - Complying with court orders or legal investigations
5. Education and Training
 - Using case studies or records for teaching, often anonymised

There are strict controls on how information is used for these purposes. These decide whether the information has to be de-identified first and whom we may share identifiable data with.

Contact the IG team (IG@combined.nhs.uk) for further information.

29. Information Security Audits

It is essential that all staff comply with the procedures put in place by the Trust 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.

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

- The protection of all records and personal information, regardless of how these are held (electronic or paper records)
- The protection of property against fraud, theft, and malicious damage
- 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 across the Trust will be subject to Information Security audits and spot-checks. The security measures of the Trust 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

In addition, 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 DPA18/UK GDPR.

Monthly checks are undertaken of all summary care record alerts and audits are undertaken on a sample of Lorenzo patient records to determine if any of the records have been inappropriately accessed. Inappropriate access of clinical records is a prosecutable offence under the Computer Misuse Act aside of the disciplinary procedures that would commence by the Trust should a staff member be found to have inappropriately accessed health records.

[Return to contents page](#)

30. Consultation and Ratification Schedule

Document Name:	Information Governance Handbook v2
Version Number:	2

Name of author:	Head of Information Governance		
Date issued:	15.04.2025		
Review date:	15.04.2026		
Target audience:	All staff including temporary staff and contractors or on behalf of the Trust		
Purpose:	To outline the standards and expectation of staffs' compliance and expected code of conduct for all staff working for the Trust		
Cross reference:	Information Governance Policies		
Contact Details for further information:	DPO@combined.nhs.uk		
Document Status			
<p>This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.</p> <p>As a controlled document, this document should not be saved onto local network drives but should always be accessed from the intranet Information governance - CAT</p>			
Version	Date	Author	Changes
1.0	14.10.2021	Liz Griffiths	
1.1	07.12.2021	Liz Griffiths	Updated CCTV and inappropriate access section
2.0	10.04.2025	Sahra Smith	Review and rewrite