Information Governance, Data Protection and Confidentiality Policy

Key points
Information Governance and Data Protection and confidentiality are consolidated frameworks for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. They provide a consistent way for employees to deal with the many different information handling requirements.

Type	Policy
Version:	5.1
Key changes since last version:	Policy placed into new template Renamed to add Information Governance to document Policy refocused to add in Information Governance aspects Definitions revised Chapter 7 has been revised to maintain data protection compliance No significant changes – removal of Information security as this is not part of our remit (separate IT security policy created by IT)
Bodies consulted:	IG Workstream
Approved by:	EMT-PAG & Information Governance Group
Date approved:	21/5/25
Lead manager:	Trust Data Protection Officer
Responsible director:	SIRO Director of Corporate Governance
Ratified by:	Policy Assurance Group
Date Ratified:	21/5/25
Date issued:	21/5/25
Review date:	May 2026
Intranet	Yes
Public website	[Usually 'No', unless patient/student facing]

Contents

1. Introduction

1.1. Information Governance and Data Protection and confidentiality are consolidated frameworks for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. They provide a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management;
- Clinical Information assurance for Safe Patient Care;
- Confidentiality and Data Protection assurance;
- Corporate Information assurance;
- Information Security assurance;
- Secondary use assurance; and
- Respecting data subjects' rights regarding the processing of their personal data.

Under the primary data protection legislation (General Data Protection Regulation (GDPR)) and Data Protection Act 2018 (DPA18), organisations that process personal data are accountable for and must be able to demonstrate their compliance with the legislation. The arrangements set out in this and related policies and procedures are intended to achieve this demonstrable compliance.

2. Purpose

The purpose of this policy is to inform Trust staff (permanent or otherwise) and students of their responsibilities related to information governance and data security, as well as the management arrangements and other policies that are in place to ensure demonstrable compliance.

This is a central policy in a suite of procedures that informs staff/students of what they should do to ensure that Trust data is:

- Held securely and confidentially;
- Processed fairly and lawfully;
- Obtained for specific purpose(s);
- Recorded accurately and reliably;
- Used effectively and ethically; and
- Shared and disclosed appropriately and lawfully.

To protect the Trust's information assets from all threats, whether internal or external, deliberate or accidental, the Trust will ensure:

- Information is protected against unauthorised access;
- Confidentiality of information is assured;
- Integrity of Information is maintained;
- Information is supported by the highest quality data;
- Regulatory and legislative requirements are met;
- Business continuity plans are produced, maintained and tested;

- Information Governance awareness training is available and mandated for all staff and students; and
- All information governance breaches, actual or suspected, are reported to, and reviewed by Information Governance team in conjunction with the Data Protection Officer (DPO)

3. Scope

3.1. All Trust staff and students are within the scope of this policy, including staff or students working in or on behalf of the Trust. For the avoidance of doubt, this includes contractors, temporary staff, embedded staff, secondees and all permanent employees

4. Definitions

Term	Definition
Consent	An indication of data subjects' wishes that is given freely and is specific, informed and unambiguous. This is a way for data subjects to signify agreement to the processing of personal data that relate to them and this can be done by a statement or by a clear affirmative action. (Article 4(11) GDPR)
Data Controller	A person who determines the purposes for and the means by which personal data are, or are to be, processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.
Data Processor	Any person (other than an employee of the data controller), who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.
Data Protection Act 2018 ("DPA")	The Data Protection Act aims to give protection to all information relating to a living individual. This includes information both processed by computers and held, stored manually in hard copy.
General Data Protection Regulation ("GDPR")	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) unifies legislation across the European Union, strengthens the data protection legislation that exists within the Data Protection Act 1998 ("DPA") and is expected to replace that Act via the new Data Protection Bill.
Data Subject	An identified or identifiable natural person who is the subject of the personal information (data).
EEA	European Economic Area.
Freedom of Information Act (2000)	The Freedom of Information Act is law giving people the general right to see recorded information held by public authorities.

Information Commissioner	The Information Commissioner is an independent official appointed to oversee the DPA and GDPR, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.
Notification	Notification is the process by which a data controller's processing details are added to a register. Under the DPA every data controller who is processing personal data needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the principles.
Personal Information or Personal Confidential Information	Data which relates to a living individual who can be identified- from those data, or from those data and other information which is in the possession of, or likely to come into the possession of the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Processing	Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.
Sensitive Personal Information	Sensitive personal data is information about a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trades' union membership, physical or mental health condition, sexual life, offences or alleged offences and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.
Subject Access Request	Under the DPA18 and GDPR, individuals can see the information about themselves that is held in electronic or physical form. If an individual wants more information on the personal data held about them, they can write to the person or organisation that they believe is processing the data, whether the data is obtained directly from data subjects or indirectly from somewhere else.

5. Policy statements

This policy aims to ensure that all Trust staff are aware of their responsibilities regarding data protection and confidentiality.
All incidents involving near misses or breaches of data protection or confidentiality are subject to local and/ or corporate review and investigation.
Data protection and confidentiality risks are managed in accordance with the Trust Risk Management Procedure.

6. Duties and responsibilities

6.1. Chief Executive

Overall accountability for procedural documents across the organisation lies with the Chief Executive. As the Accountable Officer, the Chief Executive has overall responsibility for the establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of data security and procedural documents.

6.2. Caldicott Guardian

The Caldicott Guardian:

- Ensures that the Trust satisfies the highest practical standards for handling patient identifiable information;
- Facilitates and enables appropriate information sharing and make decisions on behalf of the Trust following advice on options for lawful and ethical processing of information, in relations to disclosures;
- Represents and champions data security requirements and issues;
- Ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

6.3. Senior Information Risk Owner (SIRO)

The SIRO takes ownership of the Trust's information risk policy, acts as advocate for information risk on the Trust Board and provides assurances to the Trust's Chief Executive. The key responsibilities of the Trust SIRO are to:

- Provide a focal point for managing information risks and incidents;
- Take ownership of the assessment processes for information risk;
- Keep the Trust Board and Chief Executive up to date and briefed on all information risk issues affecting the organisation and its business partners;
- Review and agree actions in respect of identified information risks;
- Ensure that the Trust's approach to information risk is effective in terms of resource, commitment and execution, and being appropriately communicated to all staff;
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues;
- Provide leadership for Information Asset Owners (IAOs) through effective networking structures, regular scheduled meetings, sharing of relevant experience, provision of training and creation of information risk reporting structures; and
- Advise the Board on the level of Information Risk Management performance within the Trust, including potential cost reductions/associated risks and process improvements/benefits.

6.4. Information Asset Administrator (IAA)

- Information Asset Administrators ensure that policies and procedures are followed as directed by the IAO's;
- Recognise actual or potential security incidents, and consult their IAO on incident management; and
- Ensure that information asset registers are accurate and up to date.

6.5. Information Governance Team

The Information Governance team is responsible for maintaining this policy, providing advice on request to any member of staff on the issues covered within it.

6.6. Data Protection Officer (DPO)

The Data Protection Officer (DPO) for the Trust cannot be dismissed or penalised for performing his/her related tasks, does not receive any instruction from the Trust regarding exercising GDPR duties and is bound by secrecy and confidentiality. The DPO is allowed direct access to the Trust Board in matters that relates to data protection. They will:

- Inform and advise on GDPR and related obligations;
- Monitor compliance with GDPR and related obligations (including awareness raising and training);
- Provide advice about data protection impact assessment and to monitor their performance;
- Cooperate with supervisory authority (currently the Information Commissioner's Office (ICO); and
- Act as a contact point for the supervisory authority (ICO).

6.7. Senior/ Line Management Responsibilities

- Ensure all permanent and temporary staff and contractors are aware of this Information Security Policy and their security responsibilities;
- Ensure all staff using computer system have been trained appropriately;
- Ensure no unauthorised staff are allowed to access any of the Trust's computer systems or paper records;
- Ensure staff are given access to Trust computer systems based on their job role;
- Ensure all staff have fully completed the Trust employment checks;
- Ensure all staff leaving the Trust complete the staff leaver's procedures and return all Trust equipment;
- Support any information security breach investigation; and
- All external suppliers who are contracted to supply services to the Trust must have signed a Trust Confidentiality agreement, which details their legal responsibility to maintain the confidentiality of information they may come into contact with whilst working at the Trust.

6.8. Staff Responsibilities

- Each employed, contracted and voluntary staff member is personally responsible for ensuring that no breaches of data security result from their actions;
- Attend relevant data security/governance training to ensure that are fully aware of their personal responsibilities in respect of information security, and that they are competent to carry out their designated duties;
- Fully comply with the Trust's Data Security and protection policy and all relevant security policies and procedures;

- Understand that breaches of this policy will be investigated by formal disciplinary procedure which may lead to dismissal and/or legal action;
- Understand they are personally responsible for the accuracy of information/data recorded;
- Ensure they are familiar with the Trust safe haven procedures for secure transportation of information; and
- As part of their contract of employment sign a formal undertaking concerning the need to protect the confidentiality of information / observe intellectual property rights of work undertaken during the terms of employment / contract, both during and after contractual relations with the Trust.
- All staff have a duty to protect Trust IT equipment issued to them, to store it securely and not to take these items out of the country.
- To adhere at all times to the Email, Text Messaging, Apps and Internet Use Procedure in relation to the use of Trust equipment.

7. Procedures

CONFIDENTIALITY AND DATA PROTECTION

The following sections summarise key legal and national confidentiality and data protection requirements.

7.1 The Data Protection Principles

Data Protection legislation in 2018 applies to information about living individuals. It sets out six Data Protection Principles to support good practice and fairness in processing personal information. Personal Information will be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must betaken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7.1 Fair and Lawful Processing

Under the first principle of the Data Protection legislation the Trust should ensure patients are informed about the uses of and their rights regarding the processing of their personal information. This information is communicated in various ways. These materials are displayed and available in-patient waiting areas and on the Trust internet and intranet sites.
The Trust also publishes information about specific patient information sharing activities on its website (also known as a privacy notice).

7.2 Consent and recognising objections to the processing of information

An aspect of fair processing relates to individuals giving their consent for their information to be processed Explicit consent should be obtained and always recorded in cases where use of personal information would not be reasonably expected and where the information being processed is classed as particularly sensitive information. Consent is only 1 of the legal bases for sharing personal information.

For data processed for health and social care reasons (i.e., most work undertaken within the Trust) the legal basis for processing is as follows:

Article 6(1)(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and
Article 9 (2)(h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

Under Data Protection legislation, Subjects have the right to object to their personal data being processed and the Trust has a duty to ensure such objections are recorded and managed appropriately. However, there are some circumstances where an individual cannot prevent the processing of their data, e.g., reporting notifiable diseases.

Individuals also have the right for their data to be amended if it is incorrect or deleted (however the NHS must adhere to the records management code of practice for retention of medical records, which **must not** be deleted before the retention period noted in the document)

7.3 Caldicott Guardian

The Caldicott Committee Report on the review of patient-identifiable information 1997 and the subsequent Information Governance Reviews identified seven good practice principles for the health service when handling patient information:

1. Justify the purpose for using or sharing person-identifiable information.
2. Only use person-identifiable information when absolutely necessary.
3. Use the minimum person-identifiable information necessary.
4. Access to person-identifiable information should be on a strict need to know basis.
5. All staff handling person-identifiable information should be aware of their responsibilities.
6. Understand and comply with the law: Every use of person-identifiable information must be lawful.

7. The duty to share information can be as important as the duty to protect confidentiality.
8. Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Each organisation has a Caldicott Guardian (Medical Director within the Trust) who acts as the conscience of the organisation and is the most senior person responsible for patient confidentiality. It is the Caldicott Guardian's responsibility for ensuring implementation of the Caldicott principles.

7.4 Disclosure of personal information

Whether personal information can be disclosed to others is dependent on a number of factors, including, whether the patient/ service user has consented to the information being shared; to whom the information is being disclosed, and the reason for its disclosure (i.e., the legal basis for sharing). There are a number of considerations to be made when deciding whether or not to disclose information. The approach may vary according to the individual circumstances surrounding the disclosure. For example, the considerations in disclosing personal information to the police will be different to those in disclosing information for research purposes. These are explained further in the Trust Subject Access Request (SARs) Policy.

7.5 Access to Personal Information

Individuals or persons acting on their behalf with consent have a right of access to data held about them. Any person who wishes to exercise this right should make their request in writing to the Legal Services team (for patient information), Occupational Health Dept. for occupational health records or the Information Governance team (for staff information). The process for doing this is described in Trust SARs Policy.

7.6 Access to information about deceased

Data Protection legislation applies only to information about living individuals. Where the subject is deceased access to health records comes under the Access to Health Records Act 1990.

The Act permits access to records of the deceased to the legal representative of the deceased and any individual with a legitimate claim arising from the death. Though not specified in statute, duty of confidence remains applicable to the deceased and this should be considered prior to any information disclosure.

7.7 Information Security

In order to ensure the confidentiality of personal information, systems and procedures are in place to control access to such information. Such controls are essential to ensure that only authorised persons have:

- physical access to computer hardware and equipment,
- access to computer system utilities capable of overriding system and access controls e.g., administrator rights,
- access to either electronic or paper records containing confidential information about individuals.

The arrangements for the security of computer hardware, system utilities, computer files and folders are set out in the Information Security Policy and related procedures. The policy contains guidance on access controls, encryption of data, security monitoring and incidents, secure disposal of equipment and user responsibilities.

For further guidance on maintaining the confidentiality and security of personal information whilst in transit please refer to the Trust's Information Security Policy and Safe Haven Guidance.

7.8 Information Governance Incidents

7.8.1 What is a breach.

A breach is defined as:
Article 4(12) "Personal Data Breach" means a breach of security leading to the accidental destruction, loss, alteration, unauthorised disclosure, or access to, personal data transmitted, stored or otherwise processed.

The GDPR definitions, notification and subject communication requirements include incidents that organisations might not have notified under the previous data protection regime.
The traditional view that a data incident is only reportable when data falls into the wrong hands is now replaced by a concept of a 'risk to the rights and freedoms of individuals' under Article 33 of GDPR.
Any security incident that creates a risk to the rights and freedoms of the individual is a personal data incident and could be notifiable to the ICO if it reaches a certain threshold. Any personal data incident that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner via the DSPT reporting tool.

Personal data is defined as;
'any information relating to an identified or identifiable living individual' And an "Identifiable living individual" means a living individual who can be identified, directly or indirectly, by reference to— (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
This definition now makes it clear that all paper records that relate to a living individual are included in the definition and any aspect of digital processing such as IP address and cookies. Geographical data and biometric data are also clarified as being personal data when they can also be linked to a living individual.

7.8.2 What are the types of breaches:

- 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.

7.8.3 Reporting of Incidents

- All incidents will be reported on the Trust Electronic Incident Reporting system (Radar) immediately or as soon as safe to do so.
- The information reported on the incident form must be factual and accurate. No opinions or guesswork should be included. This is a legal document and must be factual.
- Staff who intentionally fail to report an incident may face disciplinary action.
- Incident reports should, wherever possible, be completed by the member of staff who first becomes aware of the incident. If that person is unable to do this due to personal injury or other circumstances the form must be completed by another person on their behalf.

7.8.3 Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner when determining what the significance and likelihood a data breach will be.

No.	Likelihood	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.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals

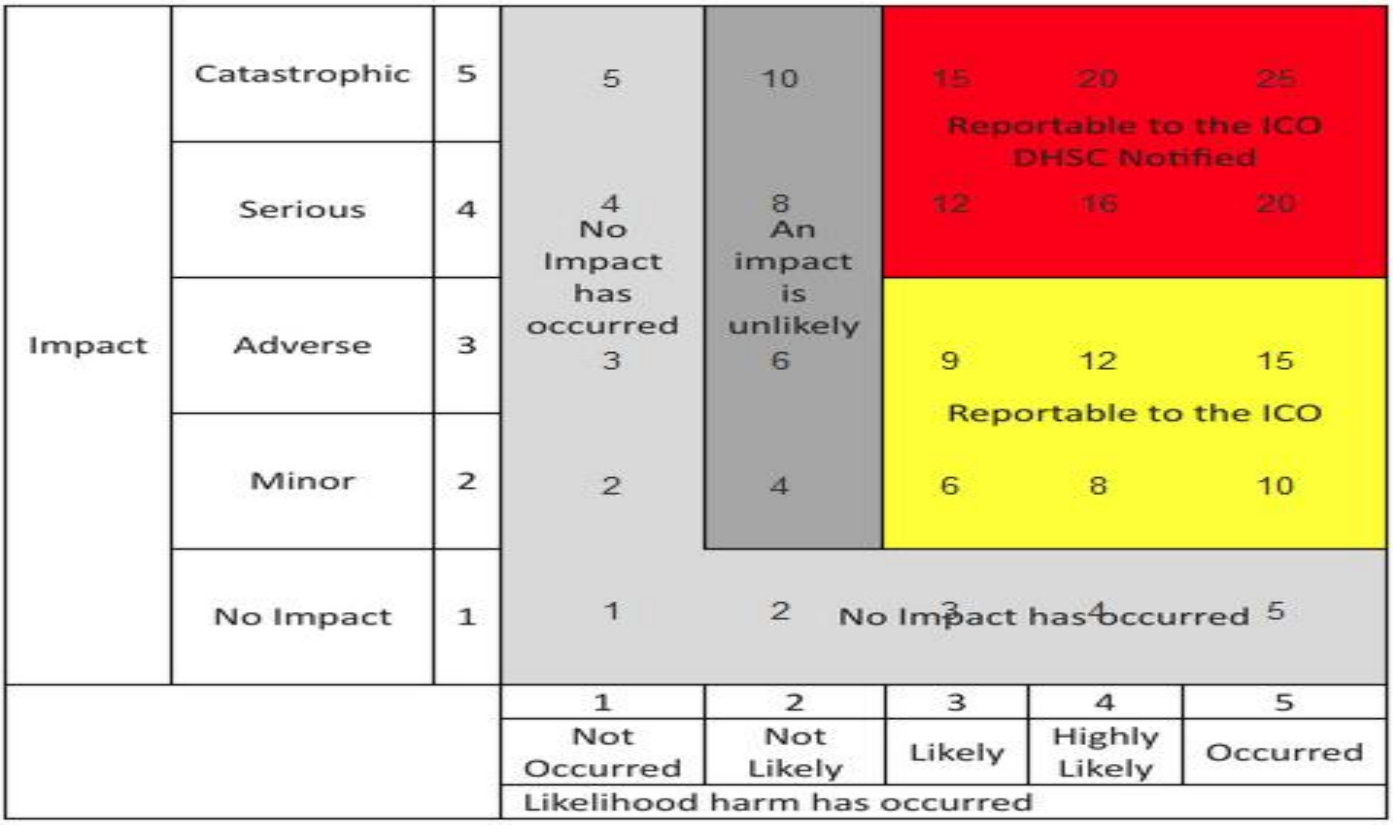
No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse

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

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

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than “green breaches” being reportable. Incidents where the grading results are in the red are advised to notify within 72 hours.



7.8.4 Duty of Candour - Being Open when Patients are Harmed

- When moderate, severe harm or death incidents occur, the Duty of Candour process must be followed. This is a clinical decision and also a contractual duty as well as being a legal duty under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 20.
- If an incident occurs which does not result in moderate or above harm the patient should still be offered an apology and an explanation given in line with being open principles. Organisations are said to be open when the prevailing culture visibly encourages key behaviours. These include honesty, openness, appropriate sharing of information and a willingness to learn from experiences to change how the organisation functions.

7.9 Audit and Monitoring

The Trust will ensure that it has assigned overall responsibility for monitoring and auditing access to confidential personal information to an appropriate senior staff member, e.g., the Caldicott Guardian and Data Protection Officer. They will ensure that the Trust has developed and implemented confidentiality audit procedures and communicating those to all staff who have access to personal, confidential data. The procedures will include:

- monitoring against NICE Clinical Guideline 138 and Quality Standard 15
- how access to confidential information will be monitored;
- who will carry out the monitoring of access;
- reporting processes and escalation processes;
- disciplinary processes.

The following are examples of events that the Trust will audit for frequency, circumstances, location etc:

- failed attempts to access confidential information;
- repeated attempts to access confidential information;
- successful access of confidential information by unauthorised persons;
- evidence of shared login sessions/ passwords;
- disciplinary actions taken.

7.9 Data Flow Mapping

The Trust is required to map all routine flows of personal information and assess associated risks. The IG team coordinates an annual review across all Trust departments of existing data flows is reviewed at least annually to meet the Data Security & Protection Toolkit and the Data Protection Officer informs the annual statutory submission to the Information Commissioner's Office in regard to processing activities and transfers of personal information outside the UK and EEA.

7.10 Retention and Storage

Records are to be retained in accordance with the NHSx Records Management Code of Practice 2023 Records, whether held in paper or electronic form must be stored securely to prevent unauthorised access. Further information regarding secure storage is available from the Information Security Policy (i.e., access controls) the Corporate Records Management Policy and Health Records Management Policy (i.e., storage and retention).

7.11 Freedom of Information

A Freedom of Information (FOI) request is when a member of the public asks for information about the Trust. The request must be in writing, does not need to state "FOI" and the sender does not need to disclose their identity. All FOI requests are processed by the Trusts' FOI lead, whose contact email is:

FOI@tavi-port.nhs.uk

8. Training requirements

A training needs analysis will be undertaken with staff directly affected by this document. Based on the findings of that analysis appropriate training will be provided to staff as necessary.
Guidance will be provided on the Trust intranet site via the communications team by Human resource (HR).
All staff will receive Data Security Awareness training via the Trust INSET days and corporate/clinical induction and will still be require to complete their Data Security and Protection Awareness training online via the Electronic Staff Record (ESR) portal and targeted training will be used where specific issues are identified.

9. Process for monitoring compliance with this policy

9.1. Compliance with the policies and procedures laid down in this document will be monitored via the corporate Data Security/Information Governance team, together with independent reviews by both Internal and External Audit on a periodic basis

The Corporate Data Security and Protection / Information Governance Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

10. References

10.1. References and Related Guidance

- Department of Health Confidentiality Code of Practice 2003
- Department of Health Records Management Code of Practice 2021
- Department of Health Information Security Code of Practice 2007
- Department of Health Caldicott Manual 2006
- BS ISO/IEC 17799:2005 and BS ISO/IEC 27001: 2005 & BS7799-2: 2005
- General Data Protection Regulation (GDPR)

- Data Protection Act 2018
- Human Rights Act 1009
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Copyright, Designs and Patents Act 1988
- Regulatory of Investigatory Powers Act 2000
- Connecting for Health Information Governance Toolkit
- The NHS Care Records Guarantee 2006
- The NHS IM&T Operating Framework
- Network and Information Systems (NIS) Regulations 2018
- Data Security and Protection Toolkit

11. Associated documents[1]

11.1. IG Management and Framework Policy v1.3

[1] For the current version of Trust procedures, please refer to the intranet.

12 Equality impact analysis

Equality Impact Assessment (EIA) Form

Equality Impact Assessments are a tool used to assess all organisational activity including policy, strategies, plans, service delivery and practice or a decision.
The general equality duty set out in the Equality Act 2010 requires public authorities, in the exercise of their functions, to have due regard to the need to:

- eliminate any form of unlawful discrimination (including direct or indirect discrimination, harassment, victimisation, and any other conduct prohibited under the Act)
- advance equality of opportunity between people who share a relevant characteristic and people who do not, and
- foster good relations between people who share a protected characteristic and people who do not.

Please refer to Equality Impact Assessment Guidance provided if you need further information.

1	**Name and Job Title of person completing the Equality Impact Assessment**	Keith James, Named Data Protection Officer
2	**Title of what you are proposing**	Amendments to the document to align to National and Legal requirements
3	**What are the main objectives or aims of what you are proposing?**	Information Governance and Data Protection and confidentiality are consolidated frameworks for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. They provide a consistent way for employees to deal with the many different information handling requirements.
4	**Date you are completing this form**	19/5/25
5	**Summary overview** *(What changes have you made following completion of the EIA?)*	No significant differential impact identified after analysis

Stage 1: Initial Screening						
6	**What evidence is available to suggest that what you are proposing will have a positive or adverse impact on people with protected characteristics or vulnerable groups?** *Please state how your proposed changes will / will not impact on the protected characteristic groups listed below. Please note: These groups may also experience health inequalities.*					
	Impact *(Positive Impact, No impact, Adverse Impact)*					**Evidence** *State below (**for each protected group**) the evidence you have used in your decision making: demographic data and other statistics including census findings, results of consultations or engagement, research findings, surveys (internal or external), complaints and compliments, incident reports, recommendations of external investigations or audit reports. Are there any key gaps in the data, evidence and findings from published or consultation documents?*
Protected Characteristics	**Positive Impact**	**No Impact**	**Low Adverse Impact**	**Medium Adverse Impact**	**High Adverse Impact**	
Age Older people; middle years; early years; children and young people.	**x**					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018

Protected Characteristics	Positive Impact	No Impact	Low Adverse Impact	Medium Adverse Impact	High Adverse Impact	
Disability Physical, sensory, and learning impairment; mental health condition, long-term conditions	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Gender Identity Inc. people who identify as Transgender	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Marriage and Civil Partnership People married or in a civil partnership	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Pregnancy/maternity Women before and after childbirth and who are breastfeeding	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Race and Ethnicity Inc. culture, history, language, traditions, ancestry, and national origin	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Religion/belief People with different religions/faiths or beliefs, or none	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Sex Women, Men	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018
Sexual Orientation Lesbian; Gay; Bisexual; Heterosexual, Gender-fluid	x					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018

*** Vulnerable groups** Populations or segments of society that are more susceptible to harm, discrimination, or disadvantage due to various factors like social, economic, or physical circumstances, requiring specific support and protection.	**x**					The policy supports all individuals by ensuring accountability is clearly defined along with obligations to support the Information Governance activity at the Trust in line with The Data Protection Act (UK) 2018

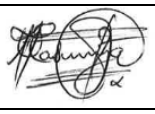
7. Human Rights (1998)
Are there any Human Rights considerations, if so, please identify which aspects (Equality Impact Assessment Guidance)

Yes *(please explain)*	
No	Not applicable in the context of this policy
Don't know	

(a) If what you are proposing is assessed as **not having impact** - Go to Section 12
(b) If what you are proposing is assessed as **having impact** - Continue to Stage 2 below.

Stage 2: Full Equality Impact Assessment Procedure			
8. **Is there service user, public or staff concerns that what you are proposing may be discriminatory, or have an adverse or positive impact on people from the protected characteristics?** *Please tick as appropriate.*			
8.1	Service users	Yes / No	No
8.2	Staff (including contractors)	Yes / No	No
No	**Can the adverse impact be justified?** *Please provide details.*		
10	**What arrangements will you put in place to monitor the impact of the proposed action or change?** *Please provide details.*		
11	**What actions will you take to address any unjustified impact and promote equality of outcome for individuals from protected characteristics.**		

Action	**Lead**	**Timescales**	**Outcome(s)**

Review Date						
Head of Culture & Inclusion Approval?	**Yes** ✓	**No**				
Name of Head of Culture & Inclusion		**Signature**		**Date of Approval**	30.07.25	

Please send completed EIAs form for review to: eia@tavi-port.nhs.uk
12. **Declaration**: I am satisfied that an Equality Impact Assessed has been completed. **Date**: 19/5/2025 **Author (name and signature)**: Keith James **Job Title**: Named Data Protection Officer
For activities that have an impact on People or have policy implications, a final copy should also be sent to the Chief People Officer: HR@Tavi-Port.nhs.uk