

Information Governance and Information Security Policy and Framework
--

Version	3.3
Designation of Policy Author(s)	Head of Information Governance and Patient Records
Policy Development Contributor(s)	None
Designation of Sponsor	Chief Information Officer
Responsible Committee	Information Governance Committee
Date ratified	14/02/2023
Date issued	01/04/2024
Review date	31/03/2025
Coverage	Trust Wide

The Trust is committed to a duty of candour by ensuring that all interactions with patients, relatives, carers, the general public, commissioners, governors, staff and regulators are honest, open, transparent and appropriate and conducted in a timely manner. These interactions be they verbal, written or electronic will be conducted in line with the NPSA, 'Being Open' alert, (NPSA/2009/PSA003 available at www.nrls.npsa.nhs.uk/beingopen and other relevant regulatory standards and prevailing legislation and NHS constitution)

It is essential in communications with patients that when mistakes are made and/or patients have a poor experience that this is explained in a plain language manner making a clear apology for any harm or distress caused.

The Trust will monitor compliance with the principles of both the duty of candour and being open NPSA alert through analysis of claims, complaints and serious untoward incidents recorded within the Ulysses Risk Management System.

CONTENTS	Page
1	Executive Summary3
1.1	Applicability and Scope3
2	Introduction3
3	Policy Objectives3
4	Definitions3
5	Duties and Responsibilities4
5.1	Committees4
5.2	Individuals4
6	Main Provisions5
6.1	General Provisions.....6
6.2	Access to Information and Information Sharing.....6
6.3	Policies the Trust will implement.....6
6.4	Information Governance Spot-check Programme7
6.5	Information Governance and Information Security Incident Management7
6.6	Staff Training and Training Standards8
6.7	Data Protection by Design and by Default.....8
6.8	Data Protection Impact Assessments9
6.9	Privacy Notices and Data Processing Documentation9
6.10	UKGDPR Principles of Data Processing9
6.11	UKGDPR individual Rights10
6.12	Lawful Basis for Processing Personal Information10
6.13	Telephone Call Recoding and Monitoring.....11
6.14	Registration with the Information Commissioner11
6.15	Authority to Act.....11
6.16	Reporting.....11
7	Key references12
8	Associated Documents12
9	Training12
10	Policy Administration12
10.1	Consultation, Communication and Implementation12
11	Appendices15
11.1	Initial Equality Impact Assessment Screening Tool15

1 Executive Summary

1.1 Applicability and Scope

- i. This policy covers all aspects of information within the organisation, including (but not limited to) patient/client/service user information, staff information and organisational information.
- ii. This Policy covers all aspects of handling information within the organisation, including (but not limited to) structured record systems (paper and electronic) and transmission of information.
- iii. This Policy covers all Information systems purchased, developed and managed by/on behalf of the Trust and any individual directly employed or any individual undertaking activity under the control or direction of the Trust.

2 Introduction

- i. The Trust regards all person identifiable information that it holds or processes as confidential and will implement and maintain policies to ensure compliance with all necessary mandatory obligations.
- ii. The Trust recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Effective information governance plays a key part in supporting clinical governance, service planning and performance management.
- iii. Effective Information Governance gives assurance to the Trust and to individuals that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.
- iv. The Trust will ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

3 Policy Objectives

- i. To provide a framework for the overall management of information processed within the Trust.
- ii. To define the actions that are required to ensure all those that are covered by the policy comply with any necessary obligations.

4 Definitions

None have been defined.

5 Duties and Responsibilities

5.1 Committees

- i. The following Committees shall be incorporated as part of the overall management of Information Governance and Information Security:
 - Information Governance Committee will provide general oversight and management of Information Governance and Information Security for the Trust.
 - The Digital Hospital Sub-Committee is the Committee to which the Information Governance committee reports to.
 - The Information Security Advisory Committee provides technical advice and assistance to the Information Governance Committee; managed tasks assigned to it and makes recommendations when asked to do so.

5.2 Individuals

- i. Senior Information Risk Owner
 - Is accountable for Information Governance and Information Security at a Trust level, which includes the risk assessment process for information risk, including review of annual information risk assessments that support and inform the Statement of Internal Control.
 - Reviews and approve actions in respect of identified information risks
 - Ensures that the organisation's approach to information risk is effective in terms of resource, commitment and execution.
 - Sets the overall objectives for Information Governance for the Trust
- ii. Caldicott Guardian
 - Is agreed as the patient's 'conscience' of the organisation who advises the Trust Board on matters relating to patient confidentiality.
 - Reviews and approves protocols governing the disclosure of patient information across organisational boundaries.
 - Approves the release of patient information where consent from the data subject is not considered necessary or appropriate.
- iii. Chief Information Officer
 - Has overall responsibility for Information Security and Information Governance
 - Ensures the overall approach taken to managing Information Governance and Information Security is appropriate
- iv. Head of Information Governance and Patient Records
 - Maintains and develops the Trust Information Governance and Information Security Policy and Framework.

- Manages Confidentiality and Data Protection across the Trust as the Subject Matter Expert
 - Implements the Information Governance related directives and objectives of the Senior Information Risk Owner
- v. Head of Technology
- Is responsible for the management of Information Security across the Trust.
 - Monitors local responses to Information Security incidents and provides support in developing proportionate and effective responses to manage information security risk.
 - Is responsible, as operational Lead, for IT services and the associated security risks.
- vi. Local Information Governance Leads
- Act as the primary departmental point of contact for Information Governance and Information Security related matters.
 - Attend the Trust Information Governance Committee meetings.
 - Co-ordinate departmental compliance to Information Governance and Information Security training and deal with any areas of non-compliance.
 - Undertake local Information Governance and Information security assessments where necessary.
 - Ensure the Information Governance Committee decisions are implemented within the area represented.
- vii. Data Protection Officer
- Informs and advises the Trust about obligations to comply with the UK General Data Protection Regulations (UKGDPR) and other data protection laws.
 - Monitors compliance with UKGDPR and other data protection laws and with relevant policies.
 - Advises on, and monitors, Data Protection Impact Assessments
 - Acts as a point of contact for the Information Commissioner's Office
- viii. Information Governance Manager
- Manages the Trust Data Security and Protection Toolkit process and submission.
 - Provides advice and guidance on compliance to mandatory standards and monitors adherence to those standards.
 - Monitors action plans related to the maintenance of, compliance with or adherence to mandatory compliance standards.
 - Is responsible for Subject Access and Freedom of Information requests.

6 Main Provisions

6.1 General Provisions

- i. The Trust places importance on the confidentiality of, and the security arrangements for, safeguarding personal information about anyone about whom the Trust processes information.
- ii. The Trust recognises the need for an appropriate balance between openness and confidentiality when processing personal information.
- iii. The Trust recognises the need to share patient information with other health organisations and other agencies in a controlled manner, consistent with the appropriate legislation and other mandatory obligations.
- iv. The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care.
- v. The Trust expects all individuals that have access to information that falls within the scope of this policy to ensure and promote the provision of this policy and any associated policy or procedure.

6.2 Access to Information and Information Sharing

- i. The Trust will implement and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking into account relevant legislation.
- ii. The Trust will implement and maintain policies to control the release of non-confidential information through the Freedom of Information Act and through the Trust Publication Scheme

6.3 Policies the Trust will Implement

- i. The Trust will implement policies covering the following:
 - The standards of conduct that it expects to be upheld for all individuals that process personal information on behalf of the Trust
 - The controlled and appropriate sharing of patient information with other agencies, taking into account relevant legislation.
 - The sharing of non-confidential information through the Freedom of Information Act and through the Trust Publication Scheme
 - The release of information to individuals through Subject Access Provisions of the UKGDPR and the Data Protection Act 2018
 - The effective and secure management of its information assets
 - The overall standards that are applied to confidentiality and data protection
 - Data Quality
 - Standards to be applied with respect to confidentiality, data protection and compliance monitoring

- ii. The Information Governance and Information Security Policy and Framework shall encompass the following:
 - Policies that relate to Confidentiality and Access to Information
 - Confidentiality Policy
 - Clear Desk Policy
 - Data Protection and Information Sharing Policy
 - Freedom of Information Policy
 - Policies that relate to Systems Access and Use:
 - Access to and the use of Clinical Systems Policy
 - Access to and the use of the Trust Network Policy
 - Acceptable Use of Email, Internet and Trust Data Policy
 - Policies that relate to the Protection of Trust Systems:
 - Physical Protection and Access Control Policy
 - Cyber Security Policy
 - Policies that relate to ensuring Service Continuity:
 - Business Continuity, Backup and Disaster Recovery Policy
 - Policies that relate to the Management of Standards and Quality:
 - Data Quality Policy
 - Audit, Compliance and Maintenance of Standards Policy
- iii. All policies covered by this policy, including this policy, shall be reviewed annually or where it is considered necessary to do so.

6.4 Information Governance Spot-check Programme

- i. The Trust will undertake an Information Governance Spot-check inspection programme to assess the compliance of departments and areas to requirements that are based on the standards set out in the Data Security and Protection Governance Toolkit.

6.5 Information Governance and Information Security Incident Management

- i. The Trust will manage incidents in accordance with the Trust incident management processes and with the:
 - “NHS Guide to the Notification of Data Security and Protection Incidents”
 - <https://www.dsptoolkit.nhs.uk/Help/29>
- ii. The Trust’s Incident Reporting system will be used to report, record, and monitor information governance and information security related incidents and risks.
- iii. Incidents will be reviewed on a periodic basis by the Information Governance Committee and Data Protection Officer.

- iv. The Trust recognises its obligations to ensure that, where an incident occurs that is of such seriousness that it is required to report the matter to the Information Commissioner's Office within 72 hours, then it will do so. The Head of Information Governance and Patient Records will be the primary contact for the Trust in respect of co-ordinating the reporting of the incident.

6.6 Staff Training and Training Standards

- i. General Training Requirements

Staff have to complete their training via one of the following methods.

Staff Group	Training Requirement	Frequency
All Staff	Data Security and Awareness training Workbook	Annual
	On-Line via NLMS/ESR	Annual

- ii. The following training is for specific staff and is in addition to the above

Department	Delivered by	Frequency
Trust Board Members	Head of Information Governance and Patient Records	2 Yearly
Information Governance Department	Head of Information Governance and Patient Records	2 Yearly
IT Department	Head of Information Governance and Patient Records	2 Yearly
Research and Development and Clinical Audit	Head of Information Governance and Patient Records	2 Yearly
Human Resources	Head of Information Governance and Patient Records	2 Yearly
Patient Records	Head of Information Governance and Patient Records	2 Yearly
Senior Information Risk Owner	Externally Sourced	2 Yearly
Caldicott Guardian	Externally Sourced	2 Yearly

- iii. Supplementary Training Requirement by Role/Responsibility

Department	Delivered by	Frequency
Information Governance Leads	Head of Information Governance and Patient Records	2 Yearly
Information Asset Owners and Delegated Information Asset Owners	Information Asset Owner Workbook or face-to-face delivered by the Head of Information Governance and Patient Records	2 Yearly

- iv. Other Supplementary Training

Training will be delivered to any department, group or individual where the Information Governance Committee, the Head of Information Governance and Records or senior management (at Deputy Director Level or above) considers it necessary.

6.7 Data Protection by Design and by Default

- i. The Trust recognises that confidentiality and data protection is fundamental to ensuring compliance to the Trust overall objectives and will incorporate “Privacy by Design and by Default” into day-to-day operational activities. This means that confidentiality and Data Protection will be a key consideration of all projects and initiatives where privacy rights are potentially impacted upon.

6.8 Data Protection Impact Assessments

- i. Data Protection Impact Assessments (DPIA) will be undertaken where the processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA will be used to assess the impact of the envisaged processing operations on the protection of personal data. This will include, but is not exclusively where the processing involves:
 - a. Systematic and extensive profiling with significant effect
 - b. Large scale processing of sensitive data, data of a highly sensitive personal nature or data concerning vulnerable individuals.
 - c. Public or systematic monitoring
 - d. Evaluation, scoring, or automated decision making.
 - e. Matching or combining datasets
 - f. The Innovative use of new technological or organisational solutions
 - g. Initiatives that would prevent individuals from exercising a right or using a service or contract.
- ii. The Trust Data Protection Officer shall be consulted on all Data Protection Impact Assessments
- iii. Data Protection Impact Assessment shall be submitted on the Trust approved template, which is available from the Information Governance Department

6.9 Privacy Notices and Data Processing Documentation

- i. The Trust will make available “Privacy Notices”, which will specify how the Trust processes the personal information it holds and will ensure that they are published on the Trust website and are also made available internally on the Trust Intranet.
- ii. The Trust will maintain an Information Asset Register, which will maintain details of the systems that hold and process personal information.
- iii. The Trust will maintain a Data Flow register, which will maintain details of instances where information is shared externally.

6.10 UKGDPR Principles of Data Processing

- i. The Trust recognises its responsibility to ensure compliance with the 6 key principles of the UK General Data Protection Regulations, Article 5 (1), that personal data shall be:
 - a. Processed lawfully, fairly and in a transparent manner in relation to individuals.

- b. 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 considered to be incompatible with the initial purposes.
- c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- e. 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 UKGDPR in order to safeguard the rights and freedoms of individuals
- f. 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.

6.11 UKGDPR individual Rights

- i. The Trust acknowledges and recognises its responsibility to give effect, where necessary, to the following 8 rights for individuals, namely the right to:
 - a. Be informed about the collection and use of personal information.
 - b. Access information which the Trust holds about individuals.
 - c. Have inaccurate personal data rectified or completed if it incomplete.
 - d. Have personal data erased.
 - e. Restrict processing or suppression of their personal data.
 - f. Data portability allowing individuals to obtain and reuse their personal data for their own purposes across different services.
 - g. Object to the processing of their personal data in certain circumstances.
 - h. Be informed if the Trust undertakes automated decisions making and profiling.
- ii. Where an individual wishes to enact their right to object to the Trust processing their personal information, and thereby wishing to opt-out of processing, the individual shall be referred to the Information Governance Department. The Information Governance Department shall refer the individual, who wishes to enact such rights, to the central NHS Opt-Out portal so that they may register that opt-out should they wish to do so, which is:
<https://digital.nhs.uk/services/national-data-opt-out>

6.12 Lawful Basis for Processing Personal Information

- i. The Trust will ensure that, where personal information is processed, there is a lawful basis to process the information, which is in line with UKGDPR Article 6 - Personal Information and UKGDPR Article 9 - Special Category (sensitive) information. Specific information relating to the lawful basis for the information processed by the Trust will be specified within the Trust Privacy Notices, which are available on the Trust website.

6.13 Telephone Call Recoding and Monitoring

- i. The Trust may implement telephone call recording. Where call recording is operating anywhere in the Trust then the Trust will ensure, so far as is reasonably practicable, that patients, staff, visitors, and other service users are made aware that their calls may be being recorded.

6.14 Registration with the Information Commissioner

- i. The Trust will maintain registration to process personal information with the Information Commissioner's Office and will pay the necessary annual registration fee in order to keep that registration current.
- ii. The Trust recognises the authority of the Information Commissioner as the Regulatory Supervisory Authority in respect of the processing of personal information, which the Trust is responsible for.

6.15 Authority to Act

- i. Approving Officers are, for the purposes of this Policy:
 - Chief Information Officer
 - Head of Technology
 - Head of Information Governance and Patient Records
- ii. Authority to vary from this policy for a specific reason and a time limited period can be given by an Approving Officer
- iii. An Approving Officer shall not be allowed to give authority where giving such authority would give rise to a conflict of interest.
- iv. Authority to vary from this Policy, which is not time-limited, may initially be given by an Approving Officer but this must then be approved by the Information Governance Committee at the first opportunity.

6.16 Reporting

- i. The Information Governance Committee shall be informed of any incidents where the cause is a systematic failure of any of its systems of control.

- ii. All Managers will provide reasonable access to any system, area or individual that will allow the Information Governance Department to assess compliance to this policy through the Spot-check Programme

7 Key references

- i. The Data Protection Act 2018
- ii. The UK General Data Protection Regulations
- iii. The Information Security Management NHS Code of Practice
- iv. The NHS Confidentiality Code of Practice
- v. The Records Management NHS Code of Practice
- vi. Freedom of Information Act 2000
- vii. Data Security and Protection Toolkit
- viii. The Computer Misuse Act 1990

8 Associated Documents

- i. Procedures:
None
- ii. Forms:
FM012 – Data Protection Impact Assessment Template
- iii. Guidance:
None

9 Training

- i. Training for implementation of this policy is contained within the Trust overall training program and is reference by Paragraph 6.6

10 Policy Administration

10.1 Consultation, Communication and Implementation

Consultation Required	Authorised By	Date Authorised	Comments
Impact Assessment			
GDPR	R Cowell	14/02/2023	None

Have the relevant details of the 2010 Bribery Act been considered in the drafting of this policy to minimise as far as reasonably practicable the potential for bribery?	Yes	
External Stakeholders		
Trust Staff Consultation via Intranet	Start date: 02/2023	End Date: 02/2023
Describe the Implementation Plan for the Policy (and guideline if impacts upon policy) (Considerations include; launch event, awareness sessions, communication / training via CBU's and other management structures, etc)	By Whom will this be Delivered?	
Publication on Intranet	Head of Information Governance and Records	

Version History

Date	Version	Author Name and Designation	Summary of Main Changes
21/08/2017	1.0	Russell Cowell, Head of Information Governance	Policy has been completely reviewed and re-written. Policy version set to version 1.0 to reflect the substantial changes and the fact that it has been developed as an integrated policy set. Previous policy set was "Information Governance Policy and Framework" and was retired as Version 8.4.
08/08/2018	1.1	Russell Cowell, Head of Information Governance	Modification to rules on training, Data Protection Impact Assessments
22/11/2018	1.2	Russell Cowell, Head of Information Governance	Renaming of 'Privacy Impact Assessments' to 'Data Protection Impact Assessments'
31/03/2020	2.0	Russell Cowell, Head of Information Governance	Major review and revision of wording considering lessons learned, introduction of new governance arrangements, insertion of GDPR definitions and provisions following independent external review by Data Protection Officer
31/03/2021	3.0	Russell Cowell, Head of Information Governance	General update to the wording to ensure the policy is kept up to date with decisions and legislation since the last update. Also reflects changes to the names of associated policies and updates to reflect changes to training requirements
30/03/2022	3.1	Russell Cowell, Head of Information Governance	Update on the requirements for Information Governance training

30/03/2023	3.2	Russell Cowell, Head of Information Governance and Records	General wording review and re-approval by Information Governance Committee. Update to job title of Head of Information Governance to add "and Records" to title. Re-allocation of policy sponsorship to the Chief Information Officer
31/03/2024	3.3	Russell Cowell, Head of Information Governance and Patient Records	General wording review and re-approval by Information Governance Committee. Minimal changes.

11 Appendices

11.1 Equality Impact Assessment

Does The Policy Affect:	Staff		Patients		Both	X
Section 1: Title of Project Proposal:	Information Governance and Information Security Policy and Framework					
Brief Description of the Project Proposal	Information Governance and Information Security Policy and Framework					
EIA Carried Out By (Name & Job Title):	Russell Cowell, Head of Information Governance and Patient Records					
Date:	14 th April 2023					
EIA Authorised By (Name & Job Title):						
Date:						
Consultation/Engagement Guidance note: How have stakeholders been consulted with? Who were the stakeholders? What level of engagement took place?	Via the Information Governance Committee					

Equality Group	Impact (Positive/Negative/Neutral)
Race (All Ethnic Group)	Neutral
Disability (Inc Physical, long term health conditions & Mental Impairments)	Neutral
Sex	Neutral
Gender Re-Assignment	Neutral
Religion Or Belief	Neutral
Sexual Orientation	Neutral
Age	Neutral

Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Other e.g., caring responsibilities, human rights etc.	Neutral

For each protected characteristic, consider whether the impact is positive. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

For each protected characteristic, consider whether the impact is negative. If so, provide supporting evidence to demonstrate how your decision was made and the impact that the policy will have with consideration of each protected characteristic (e.g., protected characteristic – impact – rationale)

Not Applicable

If your assessment has identified any negative impacts, please detail any actions that have been put in place to mitigate these (upon approval of EIA these actions will be shared with the Equality, Diversity and Inclusion Committee):

Outcome	Actions Required	Time Scale	Responsible Officer

Is there evidence that the s. 149 Public Sector Equality Duties (PSEDs) will be met? Consider whether the proposed policy will...

- Eliminate discrimination, victimisation, harassment, and any unlawful conduct that is prohibited under this act
- Advance Equality of opportunity
- Remove or minimise disadvantages suffered by people who share a relevant protected characteristic that are connected to that characteristic
- Take steps to meet the needs of people who share a relevant protected characteristic that are different from the needs of people who do not share it
- Encourage people who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such people is disproportionately low.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. (Consider whether this is engaged. If engaged, consider how the project tackles prejudice and promotes understanding - between the protected characteristics)

Explain your answers below.

The policy is an administrative policy, which implements established legal obligations neutrally.

<p>Does the EIA have regard to the need to reduce inequalities for patients with access to health services and the outcomes achieved? (this section is a requirement for any services outlined within the NHS England and Improvement Core 20 Plus 5 approach to health inequalities) Explain.</p>	
<p>The policy is an administrative policy, which implements established legal obligations neutrally.</p>	
<p>Section 2: To be completed by the EDI Manager authorising the EIA Anything for noting or any recommendations for consideration by the Board <i>Guidance Note: Will PSEDs be met? Are Core 20 Plus 5 services considering patient health inequalities?</i></p>	
<p> </p>	
<p>Review Date:</p>	<p> </p>
<p>Additional Supporting Evidence and Comments:</p> <p> </p>	