Delete as appropriate	**Policy**
DOCUMENT TITLE:	**Information Governance Policy**
DOCUMENT NUMBER:	**ELHT/C079 Version 4**
DOCUMENT REPLACES Which Version	**Version 3.1**
LEAD EXECUTIVE DIRECTOR DGM	**Director of Finance**
AUTHOR(S): Note should not include names	**Information Governance Lead/DPO**

TARGET AUDIENCE:	**All Trust Personnel**
DOCUMENT PURPOSE:	**To identify the Trusts policy to Information governance structure and reporting arrangements**
To be read in conjunction with (identify which internal documents)	

SUPPORTING REFERENCES	• **DS&P toolkit** • **Trust Corporate Risk Management Strategy** • **Other Associated IG/IS/IT policies** • **Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents** • **Informatics Planning component of the NHS Operating Framework** • **National Data Guardian standards** • **GDPR**

CONSULTATION		
	Committee/Group	**Date**
Consultation	**Information Governance Steering Group (IGSG) – chairs action**	May 2021
Approval Committee	**IGSG**	May 2021
Ratification date at Policy Council:	**October 2021**	
NEXT REVIEW DATE:	**May 2024**	
AMENDMENTS:	**Update to reflective Data Security & Protection Toolkit, Data Guardian Standards and UK GDPR**	

INFORMATION GOVERNANCE POLICY

CONTENTS

INFORMATION GOVERNANCE POLICY

1.0 Introduction

Information is an asset, which like any other business asset is extremely valuable to the Trust. Whatever form the information takes, or by whatever means by which it is shared or stored, all information must be appropriately held and protected.

The Trust recognises the importance and the necessity to have reliable and secure information, both in terms for clinical management for the delivery of care to individual service users and to corporate management for service planning and performance management.

Everyone working for the Trust has a **legal duty and responsibility** to protect and manage information in a confidential manner and to have an awareness of how information governance affects them in their daily work environment. The Trust has therefore developed and implemented a set of policies, procedures and management arrangements to provide a robust information governance framework. The Information Governance Policy is one of a set of policies that emphasises the Trusts measures to create a culture of awareness and improvement for the handling of data. This policy should not be viewed in insolation.

2.0 Purpose

This policy provides details of the Trusts framework for the implementation of the Information Governance (IG) and data protection and security Strategy to enable the Trust to meet its responsibilities in the management of information assets and resources.

The framework focuses on the management of information about patients and employees, with particular emphasis on personal and sensitive information.

3.0 Scope

This policy applies to all employees who are working on behalf of the Trust, and who are involved in the receipt, handling or the communication of person identifiable information. This policy also applies to information that is owned by other organisations which is accessed by ELHT employees.

This policy applies: -

- To all information (paper and electronic) used, managed, and shared.
- All systems purchased, developed managed by or on behalf of the Trust and its partners, including any individual directly employed or otherwise by the Trust.

- Any individual using information which is owned by the Trust.
- Any individual requiring access to information owned by the Trust.

4.0 Aims of the Policy

The Trusts Information Governance Policy has several fundamental aims: -

- To support the provision of high-quality care by promoting the effective and appropriate use of information.
- To encourage responsible staff to work closely together, preventing duplication of effort and information and enabling more efficient use of resources through better sharing practices.
- To develop support arrangements and provide staff with appropriate tools to enable them to discharge their responsibilities to consistently high standards.
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.
- To protect the Trust and its partners from information risks where the likelihood of any occurrences and consequences are significant for e.g., data losses
- To safeguard the Trusts information assets and to ensure it statutory and legal requirements are met.
- To promote a pro-active approach to information governance rather than a reactive reaction.

To achieve these aims the Trust will ensure that all information is efficiently and effectively managed on the basis of the HORUS principles i.e. that information is: -

- **H**eld safely and confidentially
- **O**btained fairly and effectively
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

The Trust recognises that there are 4 key interlinked strands to information governance: -

- Openness
- Legal compliance
- Information security
- Quality assurance

Each of these strands is covered in the Trusts information governance arrangements.

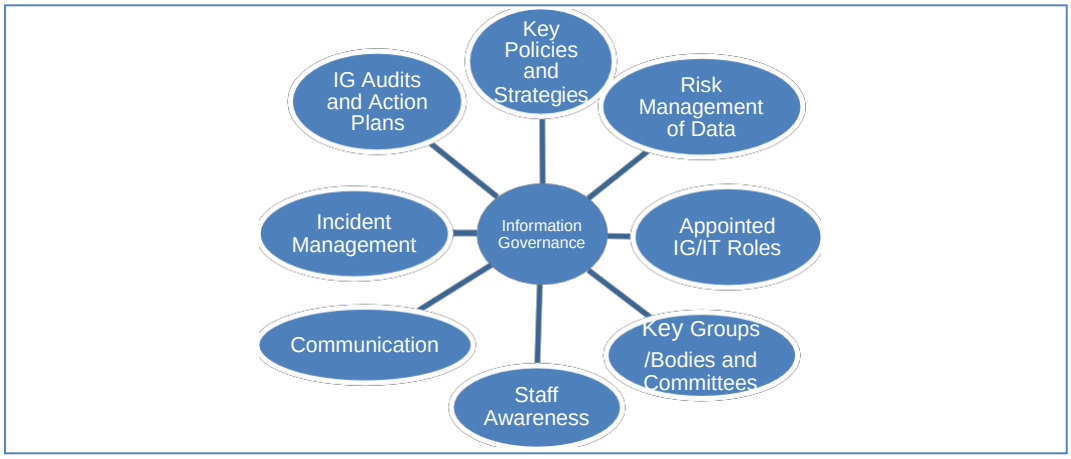
5.0 The Information Governance Framework

The Trust will implement the following best practice frameworks:

- - Data Protection Code of Practice
- The Confidentiality Code of Practice
- The Information Security Management – BS 27001/27002
- The Records Management ISO 15489 and HSC 1999/053 'For the Record'

6.0 The Trusts Information Governance Framework

The Trust will implement the strands of its adopted Information Governance Strategy: -



The deliverables of each strand are highlighted in the Trusts Information Governance Strategy.

7.0 National Data Guardian Standards

The Trust will also comply with standards set out by the office of the National Data Guardian. Compliance will be tested via additions to the Data Security and Protection toolkit and be included in CQC inspection regimes. Failure will have consequences as CCGs are obliged to ensure organisations, they contract services out to can meet these standards

National Data Guardian data security standards

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test,
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All instances of access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve any which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyberattacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken as soon as possible following a data breach or near miss, with a report made to senior management within 12 hours of detection. Significant cyberattacks are to be reported to CareCERT immediately following detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.
9. A strategy is in place for protecting IT systems from cyber threats, based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's data security standards.

8.0 The Information Governance Policy

There is a suite of Data Protection and Security polices which support this framework. This framework is aligned to NHS standards and to the requirements of the national Data Security and Protection Toolkit assessment which the Trust must ensure all standards are met on an annual basis.

A brief introduction to the Trusts Information Governance Framework can also be found in the material given to staff on induction. This summarises key responsibilities for staff whilst performing their duties in their specialised roles.

9.0 Responsibility of the Trust

The Trust, through its strategies, policies and procedures recognises its responsibilities for ensuring its robust information governance and data protection and security arrangements are well embedded into the structures of the Trust. The Trust will continue to:-

- Make the necessary arrangements to meet the performance requirements ofthe Department of Health DS&P Toolkit annual assessment.
- Report on the management of information risks within the Trusts Statement of Internal Control and to include any items of data losses and confidentiality breaches in annual reports.
- To keep updated and comply with legislation and national standards.
- Ensure that an annual audit on the trust DS&P annual submission is undertaken.

10.0 Responsibilities of Staff

Information Governance is everyone's responsibility. Staff are reminded to be aware of their legal and ethical responsibilities in handling commercially sensitive or confidential client/patient data. All employees must: -

- Read the Trusts information governance and Data Security policies as failure to comply mayresult in disciplinary action.

- To work within the principles outlined in the Information Governance Framework.
- Undertake their information governance training asap.
- Renew their DS&P training annually

11.0 Appointed Roles and Responsibilities

The Trust has appointed a series of roles and responsibilities to oversee the Trusts Information Governance and data protection and security Framework.

12.0 Key Components of the Information Governance Framework

12a. Freedom of Information and Openness

- The Trust will establish and maintain a Freedom of Information Policy to comply with the terms and conditions of the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.
- A right of access will be provided to non-confidential information about the Trust and its services through a variety of media.
- The Trust will maintain a Publication Scheme that provides a listing of documents routinely requested by the public.
- The Trust will have clear procedures and arrangements for handling queries from patients and the public and will endeavor to respond to written requests within the statutory 20 working deadline.
- The Trust will operate clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust will ensure there are established mechanisms to undertake annual assessments/audits of its policies and arrangements for openness.

Please refer to the Trusts Freedom of Information Policy for more information – Ref. C031.

12b. Data Protection and Confidentiality

- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act and UK General Data Protection Regulation 2018, the Human Rights Act 1998 and the common law duty of confidentiality.
- Patients will have a right of access to information relating to their own health care.

- Patients will have a right to exercise their data subject rights under the Data Protection Act, including the right to prevent data processing where it is unjustifiable or where it may cause harm or damage.
- The Trust regards all identifiable personal information relating to patients and staff as confidential, and any breach of confidentiality may result in staff disciplinary action being taken.
- The Trust will endeavor to keep all information secure and will undertake to commission annual assessments/audits to ensure compliance with data protection and patient confidentiality.
- The Trust regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Trust will establish a controlled framework for the appropriateness of sharing patient data with other agencies and will be mindful of its duty to disclose information for safeguarding, crime and prevention purposes under the current legislation.

12c. Fair Processing

The Trust will publish a Fair Processing Notice (FPN) informing service users of how their personal data (for example, address, name, telephone number, dob etc.) will be used, managed and shared. Service users will be advised that their personal data will only be used for the original purpose it was provided for unless consent has been gained for a second purpose or where there is an overriding piece of legislation or a provision in the Data Protection Act or GDPR that permits the data processing.

12d. Information Security

The diffusion of new technology into our daily working lives has meant that information security has become a high-level Trust Board issue. New digital systems raise risks related to information governance. There is not a day goes by where there is not another data breach published in the media.

The Trust is therefore committed to preserving the confidentiality, integrity, security and availability of its physical and electronic information assets.

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources.
- The Trust will undertake/commission annual assessments/audits to assess that its IT security arrangements are compliant with recommended standards in the NHS and NHS best practice.
- The trust will ensure a Data Protection Impact Assessment is carried out in line with requirements.
- The Trust will raise the profile of information security through its policies, procedures and IG staff training program

- The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- Business continuity and contingency plans/procedures and system access controls will be heavily monitored for the avoidance of major disruption for e.g., the avoidance of viruses and hackers etc.

Please refer to the Trust Information Security Policy for further information – ref. C045.

12e. Corporate Records Management

Good records management is paramount to enable the Trust to respond to information requests from its service users and associated partners. The Trust will therefore ensure:

- It establishes and maintains policies and procedures both for effective corporate and clinical records management.
- The Trust will adhere to the Records Management: NHS Code of Practice (Part 1: and Part 2 revised 2016) and the international Records Management ISO standard15489 as the remit for best records management practice.
- The Trust will ensure all appointed professionals are adequately trained in their specialised fields.
- The Trust will undertake annual records management audit assessments to identify better improved working practices.
- All line managers will be expected to apply effective record management practices to their service areas.

All Trust records will be expected to be classified into functional rather than organisational filing systems

Please refer to the Trusts Records Management Life Cycle policy, ref. C080 which defines roles and responsibilities and sets out the standards for records management i.e., retention schedules (which sets out retention periods for how long records should be kept), a classification scheme, and records destruction). The Clinical Records Policy ref. C103 refers to clinical case recording and clinical records management.

12f. Information Quality Assurance

Data quality is the responsibility of all staff. The Trust can only operate effectively if there is a mechanism in place to routinely and consistently check that the data we hold is fit for purpose. The quality of the services we provide as a Trust and the decisions that we make depend on the need for accurate and complete data. The Trust will therefore: -

- Establish and maintain policies and procedures for information quality assurance and the effective management of records
- Ensure there is a lead for data quality in the Trust.

- Undertake/commission an annual data quality audit to check that data standards are being maintained in accordance with national data standards,
- Seek managers to take ownership of their data to improve the quality of the information they deliver within their services.
- To promote effective data quality requirements through the Trusts IG staff training program.

The Trust will improve data quality by asking line managers and staff to report incidents of known or suspected poor-quality data. Any staff who has cause for concern over the reliability or inaccuracy of data should bring this to the attention of their line manager in the first instance.

All data audits undertaken will review the following components when determining how effective the data is: -

- The business process involved which created the data.
- The system(s) being used to support that process.
- The data being created managed or shared.
- The skills required to manage the data.
- The way in which the data is classified in the service area.

Please refer to the Trusts Data Quality Strategy, for further details.

12g. Information Sharing

An overarching information sharing protocol will be developed and maintained to provide a framework for sharing information between the Trusts partners. This framework will focus on the way personal information can be shared. This is essential to allow public sector agencies to meet their statutory obligations and the needs and expectations of our service users.

Localised information sharing agreements which operate under the framework will be prepared to outline the security arrangements for data handling and the procedures for what and how can be shared. All data sharing agreements/protocols will be approved by the Information Governance and Information Security Lead.

13.0 The Data Security and Protection Toolkit

The Department of Health DS&P Toolkit requires all NHS organisations to carry out a self-assessment of their information governance framework for compliance with against national standards.

All relevant departments will contribute to the annual submission of the Trusts DS&P Toolkit. Every department or service will provide

adequate resources to ensure that the evidence collated for the toolkit is fit for purpose.

14.0 Management Arrangements

The Trust will ensure it has an appropriate reporting structure for all related information governance issues. The Information Governance Steering Group will report to the Trust Audit Committee. Please refer to Appendix C.

15.0 Information Governance Steering (IGSG)

The Information Governance Steering Group is chaired by the Trust SIRO and will ensure it has appropriate senior representation from each service area to steer the Trust to pursue a relevant and adequate information governance and data protection and security agenda that is in line with best practice and current legislation. The Group will discuss issues relating to Data Protection, confidentiality, Freedom of information, records management, data security and information sharing.

The IG Steering Group will operate to ensure the Trust has effective policies and management arrangements covering all aspects of data protection and security.

16.0 Staff Training

It is recognised that the successful achievement of the Trust's Information Governance and data security and protection Policy and framework is dependent on the input and commitment of staff at levels in the organisation.

NHS Digital set out training requirements for all staff. The Trust Learning hub will be the main delivery method for staff to undertake their annual mandatory IG Training, but other forms of training will be available to suit staff circumstances. These are via classroom sessions or via workbook and quiz issued by the IG department

New starters will receive a brief introduction to information governance on the Trusts induction program and will be required to complete the mandatory *"An Introduction to Information Governance"* on the Trust Learning hub. Staff will be expected to complete this training annually.

Staff can also complete their annual IG training and assessment via the ELHT Learning Hub.

IG training will involve a short comprehension test. The pass rate is 80%

Those with more specialised roles within the Trust are required to undertake further additional training as documented in the IG training matrix.

The IG Lead and Team will also provide ad hoc training for SARs, FOIs and following incidents. This is important element of training for staff.

All training will be coordinated by the Information Governance Lead, who will ensure there are auditable quarterly reports to check for the completion of IG training.

17.0 Communication

The Trust will establish a robust IG communication program to raise the awareness of information governance principles to all key stakeholders and staff.

The dissemination of this Policy and framework will be through the staff intranet.

18.0 Information Governance Audits

The Information Governance Steering Group (IGSG) will receive reports from designated managers and Heads of Service who have responsibility assertions within their remit of the DS&P Toolkit.

19.0 Risk Management and Information Asset Registers

It is a core IG and DS&P objective that all information assets belonging to the Trust are identified in service/divisional information asset registers. Any residual information risks will be recorded, as per any other risk, in the Trusts division / risk registers that are managed by the divisional leads on Datix. Those risks that warrant be recorded into the Corporate Risk Register will be managed in accordance with the Trusts risk management process.

20.0 Procurement of Systems

All new systems and upgrades to existing systems, involving personal data, will be risk assessed prior to implementation or upgrade via a Data Protection Impact Assessment (DPIA). The DPIA must be completed by the system owner/project lead and submitted to IG/IS for review prior to any contracts being signed or implementation. The DPIA will be reviewed, and any identified risks dealt with accordingly by the asset owner. All/any unmitigated risks will be escalated to the SIRO and or/ICO where appropriate.

21.0 Incident Reporting

The Trust takes information risk very seriously. All information security incidents and near misses will be reported to senior management using the online Datix System. These incidents will be reported to the IGSG and will be held in a security incident log which shows the outcome, the action taken, and the further action required in respect of the incident.

In respect of data losses or confidentiality breaches, the Trust shall comply with reporting all data security incidents to the Information Commissioners Office, as appropriate, depending on the severity of the incident(s) concerned.

22.0 Information Commissioners Office (ICO)

Complainants who have an information complaint will be advised that the UK's independent regulator i.e., the Information Commissioner's Office will only independently review cases once all issues have been addressed by the Trust.

The ICO can be contacted at: -

Information Commissioner's Office
Wycliffe House
Water Lane, Wilmslow
Cheshire, SK9 5AF
Tel: 0303 123 1113 / or 01625 545
Email: casework@ico.org.uk

23.0 Policy Monitoring and Review

The effectiveness of this policy will be undertaken by the completion of an annual DS&P toolkit. This policy will be reviewed on annual basis.

Monitoring Mechanism:
Measuring and monitoring compliance with the effective implementation of this procedural

document is best practice and a key strand of its successful delivery. Hence, the author(s) of this procedural document has/have clearly set out how compliance with its appropriate implementation will be measured or monitored. This also includes the timescale, tool(s)/methodology and frequency as well as the responsible committee/group for monitoring its compliance and gaining assurance.

Aspect of compliance being measured or monitored.	Individual responsible for the monitoring	Tool and method of monitoring	Frequency of monitoring	Responsible Group or Committee for monitoring
GDPR compliance	Head of IG	Audit	Yearly	IGSG
IG Mandatory Training	Head of IG	Learning Hub	Monthly	IGSG

24.0 Dissemination and Implementation

The dissemination of this policy will be via the staff intranet

Appendix 1

Equality Impact Assessment Screening Form

Department/Function	Information Governance Department			
Lead Assessor	Head of Information Governance			
What is being assessed?	Impact of document on equality.			
Date of assessment	21.10.2021			
What groups have you consulted with? Include details of involvement in the Equality Impact Assessment process.	Equality of Access to Health Group	☐	Staff Side Colleagues	☐
	Service Users	☐	Staff Inclusion Network/s	☒
	Personal Fair Diverse Champions	☐	Other (Inc. external orgs)	☒
	Please give details: Information Governance Steering Group			

1) What is the impact on the following equality groups?		
Positive: ➢ Advance Equality of opportunity ➢ Foster good relations between different groups ➢ Address explicit needs of Equality target groups	**Negative:** ➢ Unlawful discrimination, harassment and victimisation ➢ Failure to address explicit needs of Equality target groups	**Neutral:** ➢ It is quite acceptable for the assessment to come out as Neutral Impact. ➢ Be sure you can justify this decision with clear reasons and evidence if you are challenged

Equality Groups	**Impact (Positive / Negative / Neutral)**	**Comments** ➢ Provide brief description of the positive / negative impact identified benefits to the equality group. ➢ Is any impact identified intended or legal?
Race (All ethnic groups)	Neutral	
Disability (Including physical and mental impairments)	Neutral	
Sex	Neutral	
Gender reassignment	Neutral	
Religion or Belief	Neutral	
Sexual orientation	Neutral	
Age	Neutral	

Marriage and Civil Partnership	Neutral	
Pregnancy and maternity	Neutral	
Other (e.g. caring, human rights)	Neutral	

2) In what ways does any impact identified contribute to or hinder promoting equality and diversity across the organisation?	N\A

3) If your assessment identifies a negative impact on Equality Groups, you must develop an action plan **to avoid discrimination and ensure opportunities for promoting equality diversity and inclusion are maximised.** ➢ This should include where it has been identified that further work will be undertaken to further explore ➢ the impact on equality groups ➢ This should be reviewed annually.		
Action Plan Summary		
Action	**Lead**	**Timescale**

This form will be automatically be inserted as an appendix in all Policies and Procedures which are presented for ratification at the Policy Council. Please do not hesitate to contact the qualityandsafetyunit@elht.nhs.uk if you h