East Lancashire Hospitals NHS Trust

TRUST WIDE DOCUMENT

| | |
|---|---|
| **Delete as appropriate** | **Policy** |
| **DOCUMENT TITLE:** | **Information Governance Policy** |
| **DOCUMENT NUMBER:** | **ELHT/C079 Version 3** |
| **DOCUMENT REPLACES Which Version** | **Version 2.1** |
| **LEAD EXECUTIVE DIRECTOR DGM** | **Director of Finance Information Capital and Planning** |
| **AUTHOR(S):Note should not include names** | **Information Governance Lead** |

| | |
|---|---|
| **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** | • **CFH IG toolkit**<br>• **Trust Corporate Risk Management Strategy**<br>• **Other Associated policies referenced in the document**<br>• **Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents – Gateway ref: 13177**<br>• **Informatics Planning component of the NHS Operating Framework**<br>• **National Data Guardian**<br>• **GDPR** |

| **CONSULTATION** | | |
|---|---|---|
| | **Committee/Group** | **Date** |
| **Consultation** | **Information Governance Steering Group (IGSG)** | Jan 2018 |
| **Approval Committee** | **Policy Council** | Jan 2018 |
| **Ratification date at Policy Council:** | **February 2018** | |
| **NEXT REVIEW DATE:** | **February 2021** | |
| **AMENDMENTS:** | Removal of reference to NHS digital IG training toolkit<br>Updated roles<br>Added GDPR reference<br>Added National data guardian requirements<br>Tables moved to appendices per policy council | |

# 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 has to 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) 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 IG 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

I. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

II. 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.

III. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

IV. 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 access to personal confidential data on IT systems can be attributed to individuals.

V. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

VI. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

VII. 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.

VIII. No unsupported operating systems, software or internet browsers are used within the IT estate.

IX. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

X. Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standard.

## 8.0 The Information Governance Policy/Procedure Framework

The policies and related procedures which support the Information Governance Strategy and Policy are set out in Appendix ??. This framework is aligned to NHS standards and to the requirements of the national IG Toolkit assessment which the Trust must implement.

The Trust has a comprehensive ICT framework with related formalised procedures. Users are advised to read the IG framework in conjunction with the following IT policies:-

- The Information Security Policy
- The confidentiality of Personal Data Policy
- Trust Incident Management Policy

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.

Please refer to Appendix A for an overview of the Trust Information Governance and Information Security Frameworks.

## 9.0 Responsibility of the Trust

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

- Make the necessary arrangements to meet the performance requirements of the Department of Health IG 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 Information Governance audit is regularly undertaken as part of the Trusts internal audit plan.

## 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 policies as failure to comply may result in disciplinary action.

- To work within the principles outlined in the Information Governance Framework.
- Undertake their annual/induction information governance training asap.

## 11.0 Appointed Roles and Responsibilities

The Trust has appointed a series of roles and responsibilities to oversee the Trusts Information Governance Framework. These are set out in Appendix H

## 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 endeavour 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 1998, the Human Rights Act 1998 and the common law duty of confidentiality. The Trust will also comply with GDPR and Data protection Act 2017 from May 25th 2018.
- Patients will have a right of access to information relating to their own health care, their options for treatment, subject to the exemptions and conditions of the Data Protection Act.

- 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 endeavour 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 (i.e. Health and Social Care Act, The Crime and Disorder Act, Protection of Children Act).

Please refer to the Trusts Confidentiality of Personal Information Policy – ref. C077

### 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 (where necessary). 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 raise the profile of information security through its policies, procedures and IG staff training programme.

- 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 programme.

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 Information Governance Toolkit

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

The Information Governance Lead will complete and submit the Trusts Information Governance Toolkit by 31st March each year. Every department or service will provide

adequate resources to ensure that the evidence collated for the toolkit is fit for purpose. Please refer to Appendix B.

## 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 will ensure it has appropriate senior representation from each service area to steer the Trust to pursue a relevant and adequate information governance 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. Any serious issues raised at these meetings will be escalated by the chair of the meeting, the Information Governance and Information Security Lead to the SIRO and senior management.

The Steering Group will operate to ensure the Trust has effective policies and management arrangements covering all aspects of Information Governance in line with the Trust's Information Governance Strategy and Policy.

The Terms of Reference for the IGSG can be found in the Information Governance Strategy.

## 16.0 Staff Training

It is recognised that the successful achievement of the Trust's Information Governance 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 programme 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 or.

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 outlined in Appendix C.

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 communication programme 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 for dealing with information governance requirements that fall within their remit of the IG Toolkit baseline assessment. Work programmes in all individual areas will be created by adherence to the IGTK standards and to the national standards appropriate to the individual field of activity. The Trust will aim to achieve at least level 2 performances as per Appendix B against all key assurance requirements identified in the IG Toolkit with robust improvement plans developed to address any shortfalls against any loop holes.

## 19.0 Risk Management and Information Asset Registers

It is a core IG 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 Privacy Impact Assessment (PIA). The PIA will need approval by the Information Governance department.

## 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

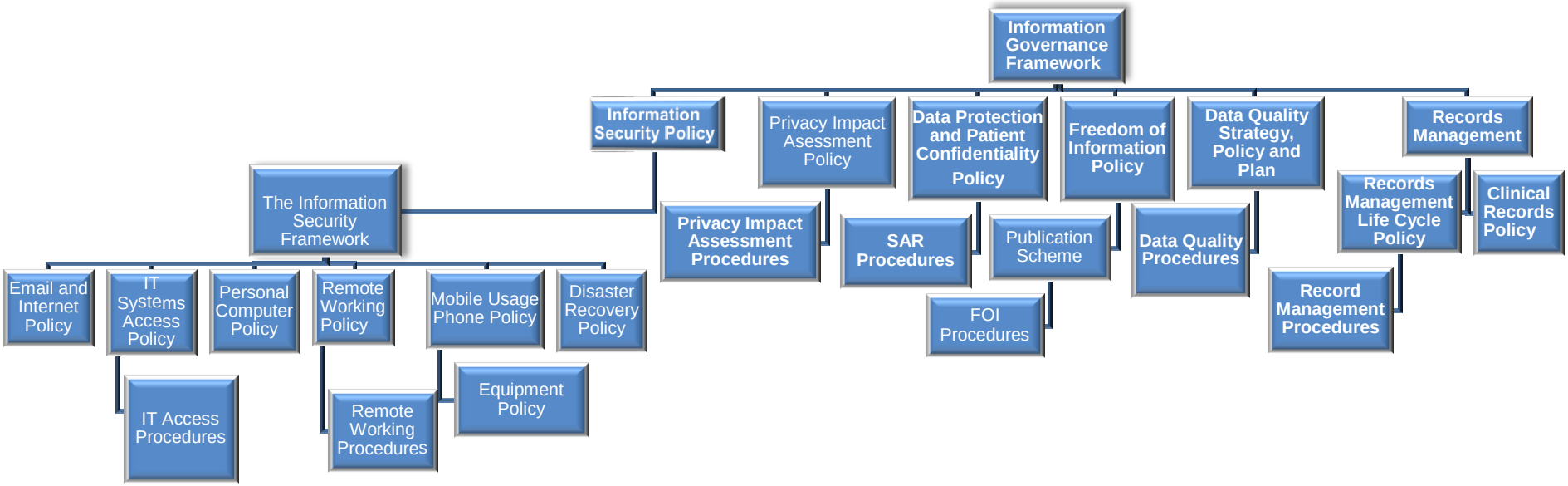
## 23.0 Policy Monitoring and Review

The effectiveness of this policy will be undertaken by the completion of an annual Information governance toolkit return in March of each year. This policy will be reviewed on annual basis. Please refer to Appendices E and F for the Trusts monitoring IG Review Plan.

## 24.0 Dissemination and Implementation

The dissemination of this policy will be through the staff intranet.

## Appendix A: The Trusts Information Governance Policy and Procedural Framework



## Appendix B: The National Information Governance Toolkit Assessment

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| **Information Governance Management** | | | | | | | | |
| 101 | There is an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda | Information Gov. Lead | √ | | | | | |
| 105 | There are approved and comprehensive Information Governance Policies with associated strategies and/or improvement plans | Information Gov. Lead | √ | | | | | |
| 110 | Formal contractual arrangements that include | Information Gov. Lead | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | compliance with information governance requirements, are in place with all contractors and support organisations | | | | | | | |
| 111 | Employment contracts which include compliance with information governance standards are in place for all individuals carrying out work on behalf of the organisation | Head of Human Resources | √ | | √ | | | |
| 112 | Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained | Information Gov. Lead /Learning &OD | √ | | √ | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | | | | | | | | |
| **Confidentiality and Data Protection Assurance** | | | | | | | | |
| 200 | The Information Governance agenda is supported by adequate confidentiality and data protection skills, knowledge and experience which meet the organisation's assessed needs | SIRO | √ | | | | | |
| 201 | The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for | Information Gov. Lead / Caldicott Guardian | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | care in an effective, secure and safe manner | | | | | | | |
| 202 | Confidential personal information is only shared and used in a lawful manner and objections to the disclosure or use of this information are appropriately respected | Information Gov. Lead | √ | √ | | | | |
| 203 | Patients, service users and the public understand how personal information is used and shared for both direct and non-direct care, and are fully informed of their rights in relation to such use | Information Gov. Lead | √ | | | | | |
| 205 | There are | Health | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | appropriate procedures for recognising and responding to individuals' requests for access to their personal data | Records Mgr. | | | | | | |
| 206 | Staff access to confidential personal information is monitored and audited. Where care records are held electronically, audit trail details about access to a record can be made available to the individual concerned on request | Information Governance Lead/Health Records Mgr. | √ | √ | | | | |
| 207 | Where required, protocols governing the routine sharing of personal | Information Gov. Lead/ Caldicott Guardian | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | information have been agreed with other organisations | | | | | | | |
| 209 | All person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines | Information Gov.Lead | √ | | | | | |
| 210 | All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, | Information Gov.Lead / Head of I.T services | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | information quality and confidentiality and data protection requirements | | | | | | | |
| **Information Security Assurance** | | | | | | | | |
| 300 | The Information Governance agenda is supported by adequate information security skills, knowledge and experience which meet the organisation's assessed needs | Head of I.T services | √ | | | | | |
| 301 | A formal information security risk assessment and management programme for key Information Assets has been documented, implemented and | Information Gov. Lead | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | reviewed | | | | | | | |
| 302 | There are documented information security incident / event reporting and management procedures that are accessible to all staff | Governance Lead | √ | | | | | |
| 303 | There are established business processes and procedures that satisfy the organisation's obligations as a Registration Authority | RA Manager | | | √ | | | |
| 304 | Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the | RA Manager | | | √ | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | terms and conditions of use | | | | | | | |
| 305 | Operating and application information systems (under the organisation's control) support appropriate access control functionality and documented and managed access rights are in place for all users of these systems | Head of I.T Services | √ | | | | | |
| 307 | An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy | SIRO | √ | | | | | √ |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| 308 | All transfers of hardcopy and digital person identifiable and sensitive information have been identified, mapped and risk assessed; technical and organisational measures adequately secure these transfers | Asst director of Performance and Information / Information Gov. Lead | √ | | | | | |
| 309 | Business continuity plans are up to date and tested for all critical information assets (data processing facilities, communications services and data) and service - specific measures | Head of Systems Support/ Information Gov. Lead | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | are in place | | | | | | | |
| 310 | Procedures are in place to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error | Head of I.T Services. | √ | | | | | |
| 311 | Information Assets with computer components are capable of the rapid detection, isolation and removal of malicious code and unauthorised mobile code | Head of I.T Services. | √ | | | | | |
| 313 | Policy and procedures are in place to ensure that Information Communication | Head of I.T Services. | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | Technology (ICT) networks operate securely | | | | | | | |
| 314 | Policy and procedures ensure that mobile computing and teleworking are secure | Head of I.T Services. | √ | | | | | |
| 323 | All information assets that hold, or are, personal data are protected by appropriate organisational and technical measures | Head of I.T Services. | √ | | | | | |
| 324 | The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where | Asst director of Performance and Information | √ | | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | appropriate | | | | | | | |
| **Clinical Information Assurance** | | | | | | | | |
| 400 | The Information Governance agenda is supported by adequate information quality and records management skills, knowledge and experience | Health Records Mgr. | √ | √ | | | | |
| 401 | There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements | Head of Systems support | √ | √ | | | | |
| 402 | Procedures are in place to ensure the accuracy of service user information on all systems and /or | Head of Systems support /Health Records Mgr. | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | records that support the provision of care | | | | | | | |
| 404 | A multi-professional audit of clinical records across all specialties has been undertaken | Health Records Mgr. | | √ | | | | |
| 406 | Procedures are in place for monitoring the availability of paper health/care records and tracing missing records | Health Records Mgr. | √ | √ | | | | |
| **Secondary Use Assurance** | | | | | | | | |
| 501 | National data definitions, standards, values and data quality checks are incorporated within key systems and local documentation is updated as | Head of Systems Support / Asst director of Performance and Information | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | standards develop | | | | | | | |
| 502 | External data quality reports are used for monitoring and improving data quality | Asst director of Performance and Information | √ | | | | | |
| 504 | improving data quality Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained | Asst director of Performance and Information | √ | √ | | | | |
| 505 | An audit of clinical coding, based on national | Head of Coding | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| IG TK Req | Area of Evidence | Responsible Lead | Director of Finance/ SIRO | Medical Director / Caldicott Guardian | Director of HR & OD | Director of Operations | Director of Service Develop't | Company Secretary/ CEO |
| | standards, has been undertaken by a Clinical Classifications Service (CCS) approved clinical coding auditor within the last 12 months | | | | | | | |
| 506 | A documented procedure and a regular audit cycle for accuracy checks on service user data is in place | Head of Clinical Audit /Health Records Mgr. | √ | √ | | | | |
| 507 | The secondary uses data quality assurance checks have been completed | Asst director of Performance and Information | √ | √ | | | | |
| 508 | Clinical/care staff are involved in quality checking information derived from the recording of clinical/care | Asst director of Performance and Information /Health Records Manager | √ | √ | | | | |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| | activity | | | | | | | |
| 510 | Training programmes for clinical coding staff entering coded clinical data are comprehensive and conform to national clinical coding standards | Head of Coding | | √ | | | | |
| **Corporate Information Assurance** | | | | | | | | |
| 601 | Documented and implemented procedures are in place for the effective management of corporate records | Trust Company secretary / SIRO | √ | | | | | √ |
| 603 | Documented and publicly available procedures are in place to ensure compliance with the Freedom of Information Act 2000 | Trust Company Secretary | √ | | | | | √ |

| | Requirement | | Information Gov. Mgt. | Confidentiality & DP Assurance | Information Security Assurance | Clinical Information Assurance | Secondary Use Assurance | Corporate Information Assurance |
|---|---|---|---|---|---|---|---|---|
| **IG TK Req** | **Area of Evidence** | **Responsible Lead** | **Director of Finance/ SIRO** | **Medical Director / Caldicott Guardian** | **Director of HR & OD** | **Director of Operations** | **Director of Service Develop't** | **Company Secretary/ CEO** |
| 604 | As part of the information lifecycle management strategy, an audit of corporate records has been undertaken | Trust Company Secretary | √ | | | | | √ |

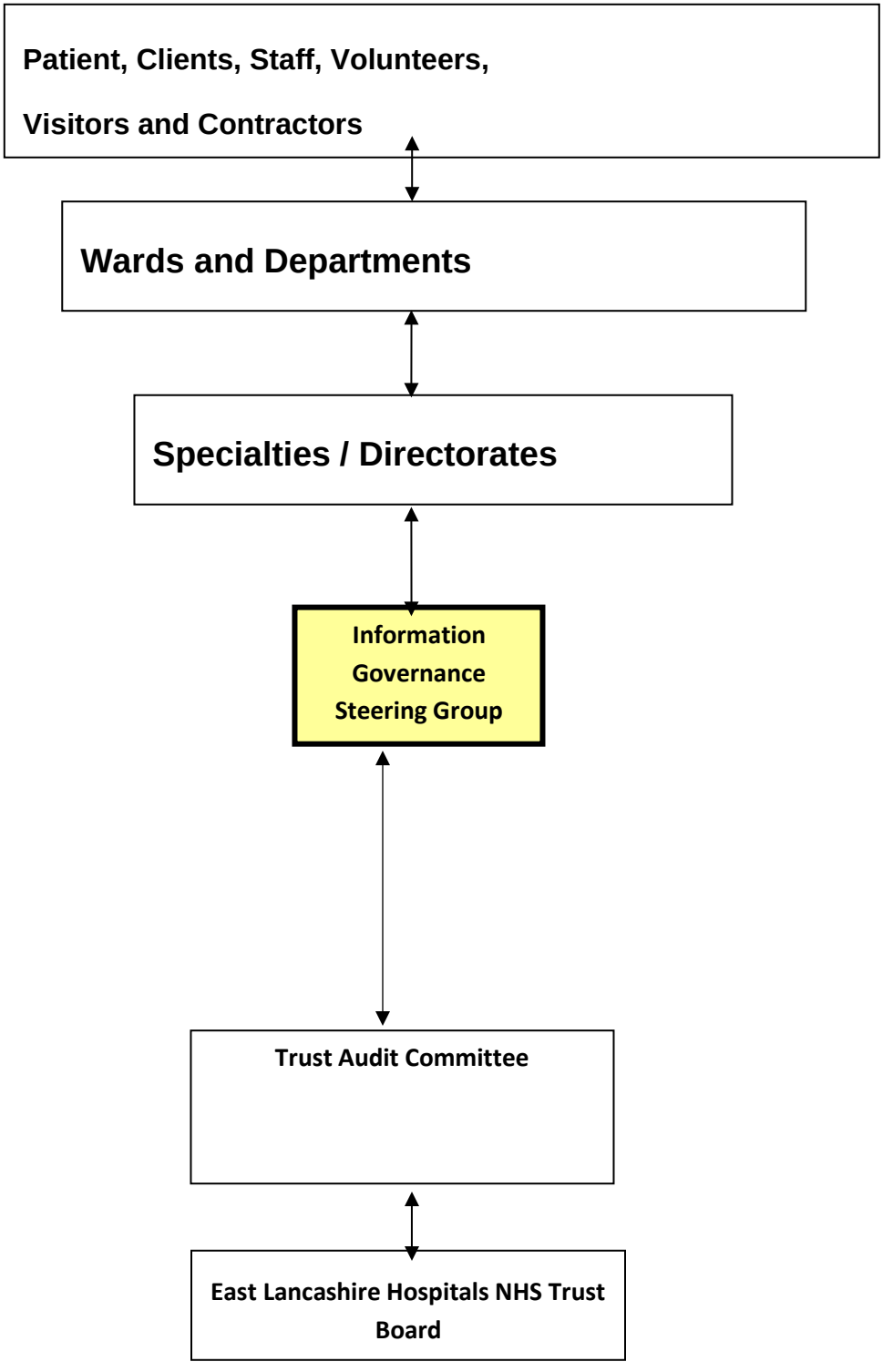
## Appendix C: – Specialist Mandatory IG Training

In addition to the Mandatory Information Governance training requirement set out in the Mandatory Training policy (HR42) the following requirement for specialist roles have been agreed **as a minimum for the role**. The minimum requirement are expected to be undertaken within 3 months of taking up the role/post

| Role | Information Governance Training | Frequency |
|---|---|---|
| SIRO | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017<br>Data Security awareness level 2 (IGTK) | 3 years |
| Caldicott Guardian | The Role of the Caldicott Guardian - Workbook - 28-03-2017<br>The Role of the Caldicott Guardian - PowerPoint - 28-03-2017<br>Data Security awareness level 2 (IGTK | 3 years |
| Company Secretary (covers FOI role) | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017<br>Data Security awareness level 2 (IGTK) | 3 years |
| Data Protection Officer | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017<br>Data Security awareness level 2 (IGTK) | 3 years |
| Head of Systems Support | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017<br>Data Security awareness level 2 (IGTK) | 3 years |
| Head of IT | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017 | 3 years |

| Role | Information Governance Training | Frequency |
|---|---|---|
| | Data Security awareness level 2 (IGTK) | |
| Health Records Manager | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br><br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017<br><br>Data Security awareness level 2 (IGTK) | 3 years |
| IAO | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br><br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017 | 3 years |
| IAA | Introduction to Risk Management for SIROs and IAOs - Workbook - 28-03-2017<br><br>Information Risk Management for SIROs and IAOs - PowerPoint - 28-03-2017 | 3 years |
| Subject Access Clerks | Training ad hoc as provided by Ig dept and external training | 2 years |
| HR Staff dealing with SARS | Training ad hoc as provided by Ig dept and external training | 2 years |

## Appendix D: Trust Reporting Structure



## Appendix E: Monitoring and Review of Information Governance Plan

| Key Elements to Monitor | Process for Monitoring | By Whom | Frequency | Responsible Group / Committee | Comment |
|---|---|---|---|---|---|
| Roles and Responsibilities | Monitored at appraisal stage and in February/March for the IG toolkit submission | IG Lead | Annually | IGSG | |
| Policies and Procedures | Monitor the Trusts statutory and legal obligations in respect of current data protection framework. | IG Lead | Annually | IGSG | |
| IG Training and its delivery | The electronic staff record will be used to identify staff who are non-compliant with IG training. | IG Support Officer and L&OD Manager | Bi-Monthly | IGSG | |
| Staff Communication Programme | An IG staff survey will be published to check if staff understand their IG responsibilities. This will determine if the communication plan needs to be tweaked. | IG Lead | Annually | IGSG | |
| Reduction of IG / Data Breaches | Bi monthly reports to determine the frequency and reason for data incidents | IG Lead | Bi -Monthly | IGSG | |
| Ensuring Best Practice Across the Trust | A range of IG audits will be undertaken to check for compliance:-<br>● DP & Confidentiality Audit<br>● IG Audit<br>● Security Audit and Reports<br>● Clinical Audit<br>● Corporate Records Management Audit | Head of IT Support &<br>Head of IG<br>Health Records Manager<br>Clinical Audit Manager | Annually | IGSG | |
| | | | | | |

## Appendix F: Bi-Monthly Review Checklist for Compliance (part of the IG Plan)

| No. | Component of the IG Toolkit | Question | Responsible Person |
|---|---|---|---|
| 1. | IG Training | What percentages of staff have completed their IG training to date? | IG Lead |
| 2. | IG Incident Reporting | How many IG incidents have been reported in the last quarter? Have these been reviewed and reported to the SIRO ? | IG Lead |
| 3. | Data Losses | Has there been any data losses of personal identifiable information (PID) associated with any information asset in the last quarter? | IAOs |
| 4. | Information Asset Register | Have all key assets been identified and are included in the Trusts information asset registers? | IAOs |
| 5. | Mobile Devices | Are mobile devices (laptops, mobiles etc.) accounted for in IT Logs? | Head of I.T |
| 6. | Allocation of Assets | Have all information assets been reviewed to check for accuracy i.e. added/removed to/from the information asset registers? | IAOs |
| 7. | Encryption | Are all mobile devices encrypted and password protected as per agreed procedures? | Head of I.T |
| 8. | Data Mapping | Have all flows of personal identifiable information been included in the service information asset registers and any associated risks identified in the risk registers? | IAOs |
| 9. | Information Sharing | Are data sharing agreements being used for the sharing of PID with external agencies? Is there a list of information sharing agreements and has this been updated recently? | IG lead |
| 10. | Fair Processing Notices | Is a fair processing notice up-to–date? | IG lead |
| 11. | Privacy Impact Assessments | When new systems and business processes are introduced are privacy impact and risk assessments been undertaken? | IG lead |
| 12. | Access Controls | Is there an up to date list of staff and contractors which have access to the Trusts information assets or has involvement in handling data from the business asset ? | Head of Systems support |
| | | | |

## Appendix G - References

- Data Protection Act 1998
- Data Protection Act 2017 (once royal assent received)
- General Data Protection Regulations (GDPR)
- Caldicott Review: Information Governance in the Health and Care System, April 2013
- Information Governance Review: To Share or Not to Share March, 2013
- Caldicott Guardian Manual, 2010
- Caldicott Report 1997
- Confidentiality: NHS Code of Practice 2003
- Health Service Circular 1999/012
- Information Security Management: NHS Code of Practice 2007
- NHS Information Governance: Guidance on Legal and Professional Obligations 2007
- NHS Litigation Agency Risk Management Standards
- Records Management: NHS Code of Practice - Part 1 2006, Part 2 2009
- International ISO Standard in Records Management 15489
- International ISO Standard in Information Security 27001/27002.

## Appendix H- Appointed Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Chief Executive (CEO) | The Trusts CEO has overall accountability for establishing and maintaining an effective information governance framework that adheres to statutory guidelines and best practice. |
| Trust Board | The Trust Board is responsible for:-<br>• Delegating this responsibility through the CEO to the Trusts SIRO.<br>• Defining the Trusts policy in respect of information governance.<br>• Ensuring there are sufficient resources allocated to support the information governance agenda in terms of staff, financial resources and senior management commitment. |
| The Senior Information Risk Officer (SIRO) | The Director of Finance, Information and Planning is the Trusts nominated Senior Information Risk Officer (SIRO). The Trusts SIRO is responsible for fostering a culture for the protection and use of data. Key responsibilities include:-<br>• To lead and champion information risk across the Trust.<br>• To oversee the development of the Trusts information risk framework.<br>• To take ownership of the risk assessment and management process for information risk and to adequately brief the Trust Board on providing written advice on the content of the Trusts internal controls.<br>• To review and agree actions in respect of identified information risks and to ensure the organisation's execution and approach to information risk is effective in terms of commitment and execution.<br>• To undertake SIRO training as and when necessary to ensure they remain effective on their role. |
| The Information Governance Steering Group | This group is responsible for:-<br>• Overseeing the day to day issues of the information governance framework;<br>• The ratification and approval of all related standard strategies, policies and procedures.<br>• To report on any exceptions to the Trust Management Committee on information Governance issues and risks.<br>• To support the SIRO and IAOs in the completion of their delegated responsibilities.. |
| Trust Secretary | The Trusts Company Secretary will oversee:-<br>• The central administration of the Freedom of information Act 2000, including responding to all information requests within 20 |

| | |
|---|---|
| | working days.<br>• The development and publication of the Trusts Publication Scheme.<br>• To undertake appropriate training, when necessary to remain effective in the role. |
| Caldicott Guardian | The Trusts Medical Director is the nominated Caldicott Guardian. The Trusts Caldicott Guardian has a particular responsibility for ensuring the use and sharing of patient identifiable information is done appropriately and securely. The role involves:-<br>• Ensuring local and national procedures and protocols are adhered to with respect to access, use of and the sharing and the transfer of patient identifiable data.<br>• To ensure that ELHT maintains the highest practical standards for lawfully and ethically handling patient data.<br>• A strategic role which champions patient confidentiality and information sharing requirements and reporting on the effectiveness of this to the IGSG and Trust Board. |
| Head of IG and Data Protection / Information Governance Lead | The Information Governance Lead will:-<br>• Provide expert advice to staff on all elements of the information governance framework.<br>• Co-ordinate and promote the awareness of Information Governance in the Trust. The team will assess the need for support and training and will ensure the information governance framework is widely disseminated to staff via the staff intranet.<br>• Establish and update all relevant strategies, policies and procedures so they are aligned to local and national standards.<br>• Develop the IG annual work plan.<br>• Provide IG support to the Caldicott Guardian and Senior Information Risk Owner (SIRO) for all internal Information Governance related issues<br>• Act as the Trusts nominated Data Protection Officer for all data protection, confidentiality and information security issues.<br>• Raise the profile of records management through effective staff communication.<br>• Monitor systems and processes for the management of all corporate records and information systems that covers all types of records.<br>• Work with all internal and external stakeholders who are responsible for data handling activities to ensure there is consistency of information governance standards across the Trust.<br>• Implement a robust information sharing framework.<br>• Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis.<br>• To complete the annual IG Toolkit assessment for the |

| | |
|---|---|
| | Department of Health and routinely report all IG assessments to the Trusts assurance processes and Committee and Trust Board structures. |
| Outpatient Reception & Health Records Manager | This role will facilitate advice and support to the Trust on clinical records management. The role will co-ordinate all clinical record activity and will ensure records are developed and maintained in an appropriate and secure manner. Responsibilities include:-<br>• Monitoring the clinical record systems and processes.<br>• Liaising with the Caldicott Guardian and the Information Governance Lead on all patient information handling activities.<br>• Raising staff awareness of the importance of clinical record keeping through appropriate use of communications and policies/procedures which are widely disseminated to staff via training and the staff intranet.<br>• Assess the need for staff support for e.g. staff training requirements.<br>• To routinely report on the performance of records management for assurance to the Health Records Steering Group and IGSG and Trust Board.<br>• Lead and manage the Subject Access Request function for the Trust. |
| Head of IT Support | The Head of IT Support will take responsibility for the physical and technical security of physical assets which lie within the IT function and other relevant departments. Key responsibilities will include:-<br>• The formulation and promotion of an IT framework i.e. the creation of policies and procedures embedded within the service area to ensure IT security arrangements are aligned to industry standards.<br>• To ensure the security accreditation of all information systems are in line with the Trusts approved definitions of risk.<br>• To be the Information Asset Owner (IAO) for the IT department with specific accountability for computer and telephone equipment and services that are operated by both corporate and clinical employees for e.g. the use of personal computers, laptops, personal digital and mobile devices.<br>• To provide compliance and to contribute towards the information security components of the IG toolkit annual assessment.<br>• To routinely provide IT assurance audit reports to the SIRO, the Information Governance Steering Group (IGSG) and the Trusts Board and Committee structures to establish that information security is adequately managed.<br>• To ensure that all IT security levels required by the Trusts Statement of Compliance are met.<br>• To assist and contribute to the development and maintenance of the Trusts information asset registers and business continuity and disaster recovery arrangements/ plans. |

| | |
|---|---|
| | • To ensure the maintenance of all firewalls and secure access servers are in place at all times.<br>• To co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach, thus involving informing the information risk lead (i.e. the SIRO), the information asset owners (IAO's i.e. the Head of Service) of the impacts, causes, outcomes resulting in particular actions and learning outcomes;<br>• To undertake specialised IT training when necessary to ensure they remain effective in their role.<br>• To configure the Trusts key network and remote access controls to mitigate against malicious or unauthorised mobile codes. |
| Information Asset Owner (IAO) | The Trusts nominated information asset owners (IAOs) will take responsibility for the assets within their service area. Each nominated IAO will be an appropriate Head of Service/DGM or/and role who has professional accountability for type of asset eg CIO will be accountable for all Information systems though the DGM will be responsible for the use of the assets within their area of responsibility. Responsibility will include:-<br>• Identifying, understanding and mitigating the information risks of each service area.<br>• The compilation of information asset registers for all key information assets within the authority of an IAO.<br>• To have an understanding of who has access to assets, and whether the asset is monitored and compliant with policy.<br>• To escalate information risks to the SIRO and the Information Governance Steering Group (IGSG).<br>• To refer any IG or IT queries to the relevant person.<br>• To be accountable to the SIRO when providing assurance on the security and use of their information assets.<br>Where there is no obvious 'owner' this will be decided by the Information Governance Lead. System ownership must be accounted for. Where a system is vested in a management forum then ownership of the facility must be decide. All system owners are responsible for determining the access policy of each system, in conjunction with advice from IT and the Information Governance and Information Security Lead.<br>System management of all systems includes:-<br>• Access protocol<br>• Auditing of user activity<br>• System validation processes (i.e. inputs and outputs etc.)<br>• Supplier support, where applicable. |
| Information Asset | Each directorate/IAO will nominate an information asset administrator to act on behalf of the information asset owner (IAO) who will take |

| | |
|---|---|
| Administrators (IAA) | responsibility for:-<br>• Updating the information risks of the service area.<br>• Conducting information risk assessments for each information asset introduced, where necessary.<br>• Identify potential or actual security incidents and consult with the IAO on incident management to ensure all information asset registers are up to date and accurate for that snap shot in time. |
| Line Managers | All line managers will ensure they:-<br>• Facilitate staff with the right advice for compliance with the Information Governance framework and policy.<br>• Promote policies and procedures to ensure the behaviour of employees is acceptable.<br>• Ensure staff complete their annual IG training assessments. |
| All Trust Staff | All staff, whether permanent or temporary (including consultants and contractors) will adhere to the Trusts policy in relation to the information governance framework. Staff will receive direction through:-<br>• The Trusts policies and procedures<br>• Staff communications and briefings<br>• Staff training<br>• Staff Intranet<br>• Head of Service/Line Manager advice |
| Third Parties | All third parties will be expected to abide by the Trusts Information Governance standards and all data protection regulations and legislation. |

## Appendix J- The Information Governance Policy/Procedure Framework

| Policy | Description of Policy |
|---|---|
| Information Governance Strategy | This strategy sets out the Trusts approach to how the Trusts Information Governance deliverables will be aligned to the requirements of NHS standards and the IG Toolkit requirements. |
| Confidentiality of Personal Information Policy – C77 | This policy lays down the principles that must be observed when dealing with access to confidential personal or business data. Staff must be aware of their responsibilities for safeguarding the confidentiality, processing and security of data in order to comply with common law obligations of the duty of confidentiality, Data Protection Act and the NHS Confidentiality Code of Practice. |
| Freedom of Information Policy – C31 | This policy sets out the roles and responsibilities of staff in relation to the Trusts obligations regarding the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. |
| Subject Access Request Policy | This policy sets out the roles responsibilities for FOI requests. |
| Registration Authority Policy | Sets out the process and roles/responsibilities for the issue and use of smart cards used to access key systems. |
| Records Management Life Cycle Policy | This policy promotes the effective management of records and the use of information within the Trust. Staff are required to recognise the importance of information as a resource for the delivery of a corporate and health services. The retention periods for all corporate records are listed in the schedules. |
| Clinical Records Policy | This policy sets out the Trusts roles and responsibilities for case recording and the management of clinical records. It outlines procedures for dealing with subject access requests and the disposal of clinical records in line with best practice retention periods. |
| Data Quality Strategy | This strategy sets out the Trusts approach to managing data accuracy for service users. |
| Information Sharing Agreement Framework | This framework sets out the processes by which the Trust will hold, process and share information in accordance with current statutory legal obligations. The framework will set out what is required to make access and the processing of data fair and lawful. |
| Information Security Policy – C45 | This policy is one of the key policies which form the Trusts Information Security Framework. It defines the information security measures required for all technology applications and the expected behaviour of staff that use the Trusts paper and electronic information assets. It sets out expectation of staff for remote and mobile working, email and PC use |