| INF3 Policy for Information Governance |
|---|
| V2 |

| | |
|---|---|
| Date Approved: | 15th October 2019 |
| Date for Review: | October 2022 |
| Directorate / Department responsible (author/owner): | Information Governance Manager |
| Contact details: | 7092 |
| Brief summary of contents | "Information Governance" covers any information relating to, and held by all departments. This will include papers, reports and minutes relating to both staff and patients. It also covers "information systems" used to hold that information. These systems may be purely paper based or be partially or totally electronic. |
| Search criteria: | Information Governance, Data |
| Executive Director responsible for Policy: | Director of Finance |
| Date revised: | October 2019 |
| This document replaces (exact title of previous version): | Information Governance Policy v1.2 |
| Title and date of committee/forum/group consulted during development : | Information Risk Management Group |
| Signature of Executive Director giving approval | |
| Intranet location: | DMS |
| Links to key external standards | - |
| Related Documents: | - |
| Training Need Identified? | None |

**Version Control Table**

| Date | V | Summary of changes | Author |
|---|---|---|---|
| 16/03/2018 | 1.1 | Update department and committee titles, clear position regarding the access to records | Paul Faulkner |
| 17.07.19 | 2 | Complete re format and update | Amanda Birkett |
| | | | |

**Document Amendment Form – minor amendments**

| No. | Date | Page no | Amendment | Authorised by |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| 10 | | | | |

Ten or less minor amendments can be made before the document is revised.

Major changes must result in immediate review of the document

If printed, copied or otherwise transferred from the Trust intranet, procedural documents will be considered uncontrolled copies. Staff must always consult the most up to date version – located on the intranet.

**Table of Contents**

## 1 Introduction and purpose

Information Governance is one of the main governance arrangements within the Trust and needs to be considered along with the other areas of governance:

- Clinical Governance
- Risk Management
- Research Governance
- Financial Governance

“Information Governance” covers any information relating to, and held by all departments. This will include papers, reports and minutes relating to both staff and patients. It also covers “information systems” used to hold that information. These systems may be purely paper based or be partially or totally electronic. The information concerned may be “owned” or required for use by the Trust and hence may be internal or external.

The governance requirements are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Trust and ensuring that relevant information is available where and when it is needed.

## 2. Scope

The aim of this policy is to provide the employees of Weston Area Health Trust with a simple framework through which the elements of Information Governance will be met.

This policy covers all types of information within the organisation, including (but not limited to):

- Patient Information
- Client Information
- Service User information
- Personnel information
- Organisational information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems - paper and electronic
- Transmission of information – fax, e-mail, post and telephone

This Policy covers all information systems purchased, developed and managed by/or on behalf of, the organisation and any individual directly or otherwise employed by the organisation.

## 3. Roles and Responsibilities

| | |
|---|---|
| Trust Board | • It is the role of the Trust Board to define the Trust’s policy in respect of Information Governance and risk and meeting legal, statutory and NHS requirements.<br>• Is responsible for ensuring that sufficient resources are provided to support the requirement of the policy.<br>• The responsibility for this is delegated through the Chief Executive Officer to the Director of Finance as Senior Information Risk Owner (SIRO). |
| Information Risk Management | • This committee is the forum for making major operational decisions and assists the Chief Executive in the performance of their duties.<br>• Development and implementation of strategy, operational plans, policies, procedures and budgets monitoring of operating and financial performance, the assessment and control of risk, prioritisation and |

| | |
|---|---|
| | allocation of resources.<br>• Receives and acts on reports from the SIRO through the Information Governance Sub Group.<br>• This Group is responsible for overseeing day to day Information Governance issues.<br>• Develop, maintain and approve policies, standard procedures and guidance.<br>• Coordinate and raise awareness of Information Governance in the Trust.<br>• Report on an exception basis to the Health Informatics Committee on information Governance issues and risk.<br>• Support the Senior Information Risk Manager in completion of their delegated duties.<br>• Direct and monitor compliance with the Department of Health Information Governance Toolkit<br>• |
| Director of Finance /Senior Information Risk Owner (SIRO) | • The Senior Information Risk Owner is responsible for and takes ownership of the organisation's information governance/risk policy and acts as advocate for information governance risk on the Board.<br>• Authorises the Information Governance Toolkit Self-Assessment submissions.<br>• Ensures that an effective information assurance governance infrastructure is in place including information asset ownership, reporting, defined roles and responsibilities.<br>• Ensures that the Information Governance Sub Group has a suitably experienced chairman in place.<br>• Ensures that there is a systematic and planned approach to the management and quality assurance of trust records. |
| Information Asset Owner (IAO) | • Information Asset Owners are senior individuals involved in running the relevant business.<br>• Their responsibility is to identify, understand and address risk to the information assets they "own".<br>• Responsible for the operational management of Trust's records in accordance with Trust policy.<br>• Accountable to the SIRO for providing assurance on the security and use of their information assets. |
| Caldicott Guardian | • The Caldicott Guardian acts in a strategic, advisory and facilitative capacity in the use and sharing of patient information.<br>• Responsible for approving, monitoring and reviewing protocols governing access to person identifiable information by staff within the Trust and other organisations both NHS and non NHS. |
| DPO | • to inform and advise employees about your obligations to comply with the GDPR and other data protection laws;<br>• to monitor compliance with the GDPR and other data protection laws, and data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;<br>• to advise on, and to monitor, data protection impact assessments;<br>• to cooperate with the supervisory authority; and<br>• to be the first point of contact for supervisory authorities and for |

| | |
|---|---|
| | individuals whose data is processed (employees, customers etc). |
| Information Governance Manager/Information Security Officer (Head of Health Informatics) | • Provides expert technical advice and guidance to the Trust on matters relating to information governance.<br>• Acts as the Trust Information Security Manager<br>• Develop and provide suitable information governance training for all staff.<br>• Monitors actual or potential reported information security incidents within the organisation.<br>• Supports and assists the IT security officer with regard to IT/information security incidents.<br>• Responsible for the timely completion and submission of the end of financial year Department of Health IG Toolkit self-assessment. |
| IT Services Manager/ IT Security Officer | • Provides expert technical advice to the Trust on matters relating to IT Security and ensures compliance and conformance.<br>• Acts as the Trust IT Security Manager.<br>• Support and assists Information Security Officer with regard to IT/information security incidents. |
| Managers | • Responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance.<br>• That all staff job descriptions contain the relevant responsibility for information security, confidentiality and records management.<br>• That staff undertake information governance mandatory training and ongoing training needs are routinely assessed.<br>• Managers shall be individually responsible for the security of their physical environment where information is processed and stored.<br>• Day to day responsibility for the management of trust records within their respective area/department |
| All staff | • All staff, whether permanent, temporary or contracted, including students, contractors and volunteers shall comply with information security policy and procedures including the maintenance of data confidentiality and data integrity and ensure that no breach of information security or confidentiality, result from their actions. Failure to do so may result in disciplinary action.<br>• All staff must ensure they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and Trust record management policies.<br>• Each member of staff shall be responsible for the operational security of the information systems they use.<br>• All staff are required to undertake relevant information governance training covering confidentiality and information security.<br>• **It is prohibited to access your own record or that of a relative unless there is urgent clinical need and can be confirmed by the line manager, failure to comply may result in formal proceedings.** |
| Third Party Contractors/ third parties | • Appropriate contracts and confidentiality/ information security agreements shall be in place with third party contractors/ third parties where potential or actual access to information assets is identified.<br>• |

## 4. Policy Details

Information Governance (IG) is considered under 6 themes:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

Information Governance contributes to the implementation of the Care Quality Commission’s Standards for Better Health. It is specifically included in standards C9 and C13:

*C9: Healthcare organisations have a systematic and planned approach to the management of records to ensure that, from the moment a record is created until its ultimate disposal, the organisation maintains information so that it serves the purpose it was collected for and disposes of the information appropriately when no longer required*

*C13: Healthcare organisations have systems in place to ensure that*
*….appropriate consent is obtained when required for all contacts with patients and for the use of any patient confidential information;*
*….staff treat patient information confidentially, except where authorised by legislation to the contrary*

It contributes to other standards (such as the NHS Litigation Authority Risk Management Standards and Audit Commission Auditors Local Evaluation) by ensuring that data required to support decisions, processes and procedures is accurate and available.

The Information Governance arrangements will underpin the Trust’s strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

Implementation of robust Information Governance arrangements will deliver improvements in information handling by following the Department of Health standards (called the “ HORUS model”), which requires information to be:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is, therefore, of paramount importance to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

This policy explains the development and implementation of a robust Information Governance (IG) framework needed for the effective management and protection of organisational and personal information.

“Information Governance” describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the Trust are sourced, held and used appropriately, securely and legally.

As a provider of health and social care, the Trust carries a responsibility for handling and protecting information of many types.

- Some information is confidential because it contains personal details of service users, their families or staff. The Trust must comply with legislation which regulates the holding and sharing of confidential personal information. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users but it is also important that personal information is not shared more widely than is necessary.
- Some information is non-confidential and is for the benefit of the general public. Examples include information about the Trust's services and information about conditions and treatment options. The Trust and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.
- The majority of information about the Trust and its business should be open for public scrutiny although some, which is commercially sensitive, may need to be safeguarded.

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 requires accurate, timely and relevant information to enable it to deliver the highest quality health care and to operate effectively as an organisation. It is the responsibility of all staff to ensure that information is complete, accurate and up to date and that it is used proactively in its business. Having complete and accurate relevant information available, at the time and place where it is needed, is critical in all areas of the Trust's business and plays a key part in corporate and clinical governance, strategic risk, service planning and performance management.

The key interlinked strands to the information governance policy are set out below:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Proactive use of information

**Openness**

- Non-confidential information on the Trust and its services should be available to the public through a variety of media, in line with the Trust's Freedom of Information (FOI) Publication Scheme.
- The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness.
- The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and, where appropriate, kept confidential, underpinning the principles of Caldicott and the regulations outlined in the EU(GDPR) Data Protection Act.
- Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust regards all identifiable personal information relating to patients as confidential.
- Compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- 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 and maintain policies and procedures to ensure compliance with the EU(GDPR) Data Protection Act, Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act.

- Appropriate training will be provided to develop the awareness and understanding of all staff with regard to their responsibilities.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable information governance controls are in place.

**Legal Compliance**

- The Trust regards all identifiable personal information relating to patients as confidential.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements.
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law confidentiality.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, The Children's Act, Computer Misuse Act).

**Information Security**

- The Trust will establish and maintain policies for the effective and secure management of its information assets, resources and IT systems.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The Trust will promote effective confidentiality, integrity and availability practices to ensure all permanent/temporary, contracted staff and third party associates of the trust adhere to this via appropriate laid down policy procedures, training and information awareness schemes/ documentation.
- 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.
- Confidentiality and integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- Information Asset Owners are expected to seek to continuously improve the quality of information held within their service
- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience in order to be able to ensure continuity in the event of system loss.
- The Trust will ensure that data anonymisation &pseudonymisation is implemented and monitored in line with Trust Policy and the NHS Operating framework 2009/2010.

**Information Quality Assurance**

- The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services, in particular data entered by their staff.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training.
- The Trust will ensure that all efforts are made to record a patient's NHS number to be used as the unique patient identifier in line with national standards.

**Proactive Use of Information**

To ensure proactive use of information, the Trust will:

- Ensure information systems hold the information required to support clinical practice and operational management.

- Develop information systems and reporting processes which support effective performance management and monitoring.
- Develop information management awareness and training programmes to support managers in using information to manage and develop services.
- Support clinical, corporate, financial and research governance requirements.
- Promote an information culture and expectation of informed, evidence-based decision making.
- Ensure that, where appropriate and subject to confidentiality constraints, information is shared with other NHS, social care and partner organisations in order to support patient care

## 5. Dissemination

The dissemination of Information Governance related topic will be coordinated by the Information Risk Management Group and actioned by the Health Informatics Service.

## 6. Implementation

The Information Risk Management Group will monitor implementation of this Policy and its associated work programmes through regular meetings and through any sub groups it establishes.

The Information Risk Management Group will review this policy every two years or in response to any significant changes to mandatory requirements, national NHS or social care guidance or as a result of significant information governance breaches or incidents.

Information Governance and Security training will be provided for all staff annually. Training will be provided as part of induction and will be a condition of connecting to the Trust's information systems.
Information Governance specialised training will be given based on job role as outlined in Appendix 1. INF3 POL Information Governance Policy v1.2
INF3 POL Information Governance Policy v1.2 Review date March 2017 Page 13 of 17

An Information Governance & Security awareness leaflet will be circulated to all staff and publicised through the Trust intranet and other communication channels.

**Information Governance Toolkit**
The Information Governance Toolkit and guidance surrounding its use will be central to the monitoring of Information Governance. An assessment of compliance with the requirements of the Information Governance Toolkit will be undertaken twice yearly as per national timetables. Action/development plans will be written and agreed by the Information Governance Committee. These plans will be monitored by the Information Risk Management Group. Final IG Toolkit submission will be presented to the Information Risk Management Group

## 7. Monitoring and Compliance

**Table 1. Mandatory Elements of Monitoring Compliance.**

| | |
|---|---|
| Element to be monitored | All elements identified within the Information Governance Toolkit will be monitored |
| Lead | Information Risk Management Group |
| Tool | Information Governance Toolkit |
| Frequency | Continuously monitor throughout the year but submission of the Toolkit is on an annual basis |
| Reporting arrangements | Will report to the Information Risk Management Group |

| | |
|---|---|
| Acting on recommendations and Lead(s) | As identified by the Information Risk Management Group |
| Change in practice and lessons to be shared | As identified by the Information Risk Management Group |

## 8. WAHT Associated Records

### Legal and Trust Related Policies

**Legal Acts**

- Data Protection Act 2018
- Human Rights Act
- Freedom of Information Act
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Computer Misuse Act
- Copyright, designs and patents Act 1988 (as amended by the Copyright Computer programs regulations 1992)
- Crime and Disorder Act
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- EU (GDPR) General Data Protection Regulations 2018
- ICO anonymisation Code of practice

**Trust Related Policies**

- IT Policies (i.e. Acceptable Use, Internet, Email Use, Portable Devices etc)
- Incident Reporting Policy
- Risk Management Strategy
- Information Security Policy
- Freedom of Information Policy
- Freedom of Information Publication Scheme
- Health Records Policy
- Electronic Patient Record (EPR) Policy
- Registration Authority (RA) Policy
- Data Protection Policy
- Data Quality Policy
- Confidentiality Policy
- Pseudonymisation and Anonymisation Policy(draft July 19)

## 9. Staff compliance statement

All staff must comply with the Trust-wide procedural document and failure to do so may be considered a disciplinary matter leading to action being taken under the Trust's Disciplinary Procedure. Actions which constitute breach of confidence, fraud, misuse of NHS resources or illegal activity will be treated as serious misconduct and may result in dismissal from employment and may in addition lead to other legal action against the individual concerned.

## 10 Equality and Diversity statement

The Trust aims to design and implement services, policies and measures that meet the diverse needs of users of our services, population and workforce, ensuring that none are placed at a disadvantage over others.

Equality Impact Assessment Screening Tool

To be completed for any procedural document when submitted to the appropriate committee for approval.

| | | Yes/No | Rationale |
|---|---|---|---|
| 1 | Does the policy/guidance affect one group less or more favourably than another on the basis of: | | |
| | • Race | No | |
| | • Ethnic origins (including gypsies and travellers) | No | |
| | • Nationality | No | |
| | • Gender | No | |
| | • Culture | No | |
| | • Religion or belief | No | |
| | • Sexual orientation | No | |
| | • Age | No | |
| | • Disability - learning disabilities, physical disability, sensory impairment and mental health problems | No | |
| 2 | Is there any evidence that some groups are affected differently? | No | |
| 3 | If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? | No | |
| 4 | Is the impact of the policy/guidance likely to be negative? | No | |
| 5 | If so can the impact be avoided? | No | |
| 6 | What alternatives are there to achieving the policy/guidance without the impact? | No | |
| 7 | Can we reduce the impact by taking different action? | No | |
| 8 | Actions identified following screening process | None | |
| 9 | Screening identified a full impact assessment. | No | |

If you have identified a potential discriminatory impact of this policy/procedure, please refer it the appropriate Director in the first instance, together with suggested actions required to avoid/reduce this impact. For advice in respect of answering the above questions, please contact the H.R Department. For advice on completion of this form please contact the Governance Team.

## Appendix 1 - Information Governance Training Needs Analysis

Introduction Information is an extremely valuable resource and is essential for the delivery of high quality services. Good Information Governance (IG) practices ensure necessary safeguards for the appropriate use of business and Personal Confidential Data (PCD) are in place and managed effectively. These safeguards can be found in the policies and procedures applicable to all staff but of equal importance is the knowledge and awareness each individual maintains of IG to recognise and work within these safeguards.

Therefore it is a mandatory requirement that all staff including permanent, temporary, contractors and agency staff will receive appropriate basic Information Governance Training and to have that training refreshed annually.

While there is already an existing requirement within the IG toolkit to annually complete IG training. The importance of this training was also clearly recognised in with recent Caldicott Review 2 which states:

**'All staff should receive annual basic Information Governance Training appropriate to their role'**

The IG training requirement also requires that:

- Basic IG training is provided for all new starters as part of their induction; and
- Additional training is provided to staff in key roles

Training delivery for the trust is detailing in the IG strategy within the Training Plan.

### Information Governance Training Needs Analysis Matrix

All members of staff including permanent, temporary, contractors, agency staff and work placements must complete the mandatory training modules detailed below and in accordance with the following:

- New starters/returning to work, are required to complete within their first 10 working days of starting or returning to work,
- Staff having completed their introduction or beginner's guide modules only need to complete the 'Refresher module' in subsequent years, All other TNA modules are to be completed annually unless otherwise informed,
- All staff must maintain a valid 12 month basic mandatory training pass.

ALL STAFF ARE REQUIRED TO COMPLETE THE MANDATORY MODULE AS DETAILED IN THE ‘ALL STAFF’ JOB ROLE BELOW

| **Job Role** | **TNA Modules to complete** |
|---|---|
| ALL STAFF regardless of role | MANDATORY: Introduction to Information Governance (Year 1) followed by the refresher module **Annually** |
| Admin and Clerical (access to PCD) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act □ Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Admin and Clerical (no access to PCD) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Caldicott Guardian | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches<br>• Caldicott & SIRO Annual Refresh |
| Senior Information Risk Owner (SIRO) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |

| **Job Role** | **TNA Modules to complete** |
|---|---|
| ALL STAFF regardless of role | MANDATORY: Introduction to Information Governance (Year 1) followed by the refresher module **Annually** |
| | • Caldicott & SIRO Annual Refresh |
| Clinical Staff | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Information Governance Lead or Support | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches<br>• And all applicable modules<br>• Caldicott & SIRO Annual Refresh |
| Corporate Records Management Leads | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Information Asset Owner (IAO) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice |

| Job Role | TNA Modules to complete |
|---|---|
| ALL STAFF regardless of role | MANDATORY: Introduction to Information Governance (Year 1) followed by the refresher module **Annually** |
| | • Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Information Asset Administrators (IAA) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Staff dealing with Subject Access Requests (PCD) | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Freedom of Information Lead and Support Staff | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018<br>• NHS Data Breaches |
| Business Intelligence staff | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018 |

| **Job Role** | **TNA Modules to complete** |
|---|---|
| ALL STAFF regardless of role | MANDATORY: Introduction to Information Governance (Year 1) followed by the refresher module **Annually** |
|  | • NHS Data Breaches |
| IT staff | • Give you an understanding of Information Governance<br>• What we need to do to make Information Governance work<br>• Confidentiality<br>• Who to go to for support<br>• Smart cards<br>• Freedom of Information Act<br>• Records Management NHS Code of Practice<br>• Caldicott Guidelines<br>• EU(GDPR)Data Protection Act 2018 |