Policy Document Control Page

Title
Title: Information Governance Policy

Version: 6

Reference Number: CO44

Keywords:
Information Governance

Supersedes
Supersedes: Version 5
Description of Amendment(s): Minor updates -

- **Responsibility and Accountability – inclusion of IAMs**
- **Linked Policy list updated**
- **Update regarding Training**

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Paul Byrne

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Jonathan Mayes
ERA undertaken on: 16th August 2011
ERA approved by EIA Work group on: 16th August 2011

Where policy deemed relevant to equality-
EIA undertaken by Jonathan Mayes
EIA undertaken on 16th August 2011
EIA approved by EIA work group on 16th August 2011

Approval and Ratification

Referred for approval by: Paul Byrne

Date of Referral: 11th November 2015

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date Ratified by Executive Directors: 20th March 2017

Executive Director Lead: Director of Service Development and Sustainability

Circulation

Issue Date: 23rd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? YES

Review

Review Date: March 2018 (or as changes are required as a result of GDPR).

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 23rd March 2017

Contents Page

Information Governance Policy

1.0 Introduction

1.1 'Information Governance (IG) allows organisations to ensure that personal information is handled legally, securely, efficiently and effectively in order to deliver the best possible care'.

1.2 This Policy sets out the approach to be taken within the Trust to provide relevant Groups and the Board with assurance that a robust Information Governance (IG) framework and associated work programme is in place.

1.3 Information is a vital asset, both in terms of the clinical management of individual service users and the efficient management of services and resources. It plays a key part in all areas of the Trust's operations including (but not restricted to) delivering healthcare to service users, Clinical Governance, Risk Management, Corporate Governance, Informatics, Service Planning and Delivery and Performance Management and Business Intelligence.

1.4 IG affects **ALL** employees, contractors and anyone providing a service on behalf of the Trust, whether permanent or temporary. **EVERYBODY** has responsibilities for IG on a day-to-day basis, whether they work in a clinical or non-clinical environment. Contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these.

1.5 It is of paramount importance to ensure that information is efficiently and legally managed and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

1.6 IG encompasses legislation and guidance including the Data Protection Act 1998; Freedom of Information Act 2000; Environmental Information Regulations 2004; Records Management Code of Practice 2016; Information Security Code of Practice ISO 270001; Regulation of Investigatory Powers Act; Confidentiality Code of Practice; Health and Social Care Act 2016; and the Human Rights Act 1998.

1.7 In addition to the regulatory aspects, there are also ethical aspects to consider, including service user choice, human rights and best interest.

2.0 Scope

2.1 This Policy covers all aspects of information within the organisation, including (but not limited to):

- Employee/Client/Service User clinical information
- Personnel information
- Organisational information (e.g. financial, Payroll, HR)

2.2 This Policy covers all aspects of handling (processing) the way the Trust holds, obtains, records, uses and shares information, including (but not limited to):

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

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

2.4 This policy should be read in conjunction with all relevant policy and procedure as outlined at section 11.3.

3.0 Responsibility and Accountability

3.1 The Trust Board

3.2 The Health and Social Care Information Centre (HSCIC) stipulates that all NHS Trusts should have in place appropriate lines of accountability for IG throughout the organisation. For this Trust, the Chief Executive, supported by the Trust Board has overall strategic accountability for IG, the completion of the annual baseline assessment and any associated work programme, including the maintaining of an appropriate policy and procedure suite and relevant IG and Information Risk frameworks.

3.3 To fulfil its obligations, the Board has delegated authority for IG to the Integrated Governance Group, and operationally to the Information Governance Assurance Group.

3.4 The Caldicott Guardian and Senior Information Risk Owner (see below) are both members of the Trust Board.

3.5 Senior Information Governance and Risk Officer

3.6 All NHS Trusts are required to have a Senior Information Risk Owner (SIRO) who is nominated by the Chief Executive and who should be a member of the Trust Board. The SIRO has responsibility for ensuring compliance with legislation and national policy in relation to the security of information, in particular person identifiable information.

3.7 The Trust SIRO is the Director of Service Development and Sustainability.

3.8 Further details of the key responsibilities of the SIRO can be found at Appendix A.

3.9 Caldicott Guardian

3.10 The Caldicott Guardian (CG) plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient identifiable information. Acting as the ‘conscience’ of the Trust, the CG also supports work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information, as required.

3.11 The Trust Caldicott Guardian is the Medical Director.

3.12 **Line Managers / Senior Managers**

3.13 All Line Managers have responsibility to ensure that staff are compliant with and working to all relevant policy and procedures in relation to Information Governance, and completion of all relevant IG training modules. They also have responsibility for ensuring any incidents or policy breaches in relation to IG principles are reported immediately.

3.14 **All employees and contractors, and anyone providing a service on behalf of the Trust.**

3.15 All employees and contractors of the Trust, whether permanent, temporary or contracted, have responsibilities for IG on a day-to-day basis, whether they work in a clinical or non-clinical environment. Contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these. Any incident involving a breach or suspected breach of the Data Protection Act (DPA) shall be reported to their line manager immediately and, where they are not available, to the Trust's Information Governance Manager or Senior Information Governance and Risk Officer

3.16 **Information Governance Manager**

3.17 The Trust's Senior Information Governance and Risk Officer shall ensure the Trust complies with all legislation and NHS Policy in relation to Data Protection, Freedom of Information, Records Management, Caldicott, Confidentiality and Information Security. The IG Manager shall ensure the function is adequately resourced and shall report any identified weaknesses or risks to the Trust IG compliance to the SIRO and ultimately the Trust Board.
The IG Manager is responsible for ensuring the management of the Information Governance Assurance Group.

3.18 **Information Risk Manager**

3.19 The Trust's Information Risk Manager shall have responsibility for implementing robust information risk management throughout the Trust, ensuring compliance with legislation and national policy in relation to the management of information risk.

3.20 **Records Managers**

3.21 The Trust's Records Managers are responsible for the overall development and maintenance of records management practices throughout the organisation. In particular, the Records Managers are responsible for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

3.22 **Information Asset Owners (IAOs)**

3.23 The Trust's Information Asset Owners (IAOs) support and drive the information governance agenda and provide the Trust Board – via the SIRO – with the assurance that effective Information Governance best practice mechanisms are in place within the Trust.

3.24 Information Asset Owners (IAOs) are Board-level/Director/very senior management level members of staff who have overall accountability for the assets within the services under their remit. They will assist in identifying strategic threats and vulnerabilities, both internally and externally, to their services (and as such their information assets), and will advise on the impact such risks would have at a strategic level. They will have an understanding of the strategic value of each asset within their service, and – with the assistance of the Information Asset Managers – will identify critical assets within their remit.

3.25 They shall also ensure that information risk assessments are reviewed each quarter on all information assets where they have been assigned 'ownership', following guidance from the Senior Information Governance and Risk Officer.

3.26 The IAOs report directly to the SIRO, and will be responsible for nominating appropriate Information Asset Managers for each information asset.

3.27 **Information Asset Managers (IAMs)**

3.28 Information Asset Managers (IAMs) are Service/Department Manager level staff and will coordinate the identification of information assets within their remit and will assign an Information Asset Administrator for each asset.

3.29 The IAM will have a thorough understanding of their information assets; their importance to the organisation, their links and dependencies on other assets, tactical threats and vulnerabilities facing the assets, and the direct and indirect impact these risks would have on the Trust.

3.30 The IAM will nominate an appropriate IAA for each information asset.

3.31 **Information Asset Administrators (IAAs)**

3.32 The Trust's Information Asset Administrators (IAAs) can be any member of staff with an in-depth working knowledge of the asset and data flows, ideally Operational Manager (e.g. supervisor or team leader), but can be any officer, as appropriate. The IAA will have a thorough understanding of how the asset is used on a day-to-day basis, and how and when information is added and removed from the asset.

3.33 IAAs ensure that policies and procedures are followed regarding their asset. They will proactively and reactively recognise actual or potential security incidents, and will consult their IAO/IAM regarding incident management. They will assist in the identification of threats and vulnerabilities within the asset, documenting the flow of their assets, and in determining the value of their asset.

4.0 Strategic development of IG

4.1 This Policy cannot be implemented in isolation as the management of information plays a key part in all areas of the Trust's operations including (but not restricted to) Clinical Governance, Risk Management, Corporate Governance, Informatics, Service Planning and Delivery and Performance Management and Intelligence. This Policy, therefore, links into all aspects of the organisation and is to be implemented in conjunction with other specific Trust strategies. IG will be represented on the agenda of any other Trust groups, committees, or the Board, as well as on partner organisations and other agency groups, as appropriate.

5.0 Policy Objectives

5.1 This Policy has been created to:

5.2 Protect the Trust, its staff and its service users from information risks where the likelihood of occurrence and the consequences are significant.

5.3 Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes.

5.4 Encourage pro-active rather than re-active information risk management.

5.5 Provide assurance to the Trust Board and improve the quality of decision making throughout the Trust.

5.6 Meet legal or statutory requirements.

5.7 Assist in safeguarding the Trust's information assets**.**

6.0 Principles of IG Management

6.1 Accurate, timely and relevant information is essential to deliver the highest quality health care to service users. 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 service user and, in some circumstances, the public interest.

6.2 However, the Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

6.3 The Department of Health has set standards that should be adhered to in ensuring that information is:

- Held Securely and Confidentially
- Obtained Fairly and Efficiently
- Recorded Accurately and Reliably
- Used Effectively and Ethically
- Shared Appropriately and Lawfully

7.0 Aspects of the Trust Information Governance agenda

7.1 Openness

- Information will be defined and, where appropriate, kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act 1998
- Non-confidential information on the Trust and services will be available to the public through a variety of means, in compliance with the Freedom of Information Act 2000
- Service users should have ready access to information relating to their own health care, their options for treatment and their rights as service users. There should be clear procedures and arrangements for handling queries from service users and the public
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media

7.2 Legal Compliance

- The Trust regards all identifiable personal information relating to service users or staff 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 1998, Human Rights Act 1998 and the Common Law Duty of Confidentiality
- The Trust will establish and maintain protocols for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998, Protection of Children Act 1999)

7.3 Information Security

- The Trust will establish and maintain policies for the effective and secure management of its information assets and resources
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust’s Incident Reporting system and Risk Management processes will be used to report, monitor and investigate all breaches of confidentiality and security.

7.4 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
- 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

8.0 External Assessment

8.1 It is mandatory for the Trust to submit an annual HSCIC IG Baseline Assessment, which is completed via the HSCIC IG Toolkit. The assessment criteria evolve annually to reflect the national IG agenda. Further information on the toolkit can be found via https://nww.igt.hscic.gov.uk/

8.2 In addition to the IG Baseline Assessment, IG forms part of other internal and external scrutiny regimes including Care Quality Commission standards, NHSLA, The Care Record Guarantee, the Trust Annual Report and IG Statement of Compliance.

8.3 The Trust baseline assessment and IG compliance is subject to regular monitoring and audit by the Internal Audit and ad hoc by the Strategic Health Authority.

8.4 The Trust annually submits its Data Protection registration with the Information Commissioners Office (ICO), who has regulatory responsibility for ensuring compliance with the DPA and investigating any suspected or reported breach. Where an organisation is found guilty of a breach, severe financial penalties may be imposed. The Trust Data Protection Policy provides more details.

9.0 Incident Reporting and Management

9.1 All employees, contractors and anyone providing a service on behalf of the Trust have responsibility to immediately report any incident involving the known or suspected loss, damage or misuse of information in paper or electronic form. Any incident should be reported via the Trust’s incident reporting system.

9.2 The Trust has a responsibility to investigate any IG incident in order to protect its service users. Any investigation will be carried out in accordance with the Trust’s Incident Reporting protocols and the Incident Reporting, Management and Investigation Policy.

10.0 Development and Management of the IG programme

10.1 The Trust is required to undertake a baseline assessment of IG compliance utilising the HSCIC IG Toolkit by 31st March each year and produce an IG work plan based upon the results. There is an expectation that year on year improvements will then be made and these will be reported via the IG Toolkit.

11.0 Further Information or Help with Information Governance

11.1 This Policy is designed to provide an overview of the Trust’s IG assurance tool. If you would like further information about Information Governance, visit the NHS Connecting for Health Website: http://systems.hscic.gov.uk/infogov where you can download a copy of 'What you should know about Information Governance'. Alternatively, contact the Senior Information Governance and Risk Officer via email or telephone.

11.2 All conversations/requests with the Information Governance Manager and Information Risk Manager will be treated confidentially.

11.3 This Policy should be read in conjunction with relevant and overlapping policies and Strategies including (but not restricted too):
Information Governance Staff Handbook
Data Protection Policy
Information Governance Policy
Information Security Policy
Access to Health Records
Freedom of Information Policy
Information Risk Management Policy
Information Sharing Policy
Records Management Policy
IG Requirements for New Processes and Systems
Environmental Impact Regulations

12.0 Training

12.1 All employees, contractors and anyone delivering a service on behalf of, or working to the Trust as required to complete IG training akin to their role and responsibility.

12.2 It is the responsibility of all managers and recruiting officers to ensure everyone completes at least the minimum IG training consummate to their role.

12.3 The IG training requirements are laid down in the ‘Information Governance Training Plan.’ There are various elements of IG training, including the mandatory annually. For further information see Appendix C.

13.0 Review

13.1 This Policy shall be reviewed within 12 months of its ratification. Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

14.0 Contacts within the Trust

14.1 SIRO – Director of Service Development and Sustainability
Caldicott Guardian – Medical Director
Information Governance Manager
Senior Information Governance and Risk Officer
Information Asset Owners (See Appendix B)

Appendix A

SIRO – Key Responsibilities

1. Policy and process

- Oversee the development of an Information Governance Policy. This should include a Strategy for implementing the policy within the existing Information Governance Assurance Framework and be compliant with NHS IG policy, standards and methods.
- Take ownership of the assessment processes for information risk, including cyber security, including prioritisation of risks and review of the annual information risk assessment to support and inform the Statement of Internal Control.
- Understand the strategic goals of the Trust and Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners.
- Review and agree actions in respect of identified information risks.
- Ensure that the Organisation's approach to information risk is effective in terms of resource, commitment and execution, being appropriately communicated to all staff.
- Provide a focal point for the escalation, resolution and/or discussion of information risk issues.
- Ensure that an effective infrastructure is in place to support the role by developing a simple Information Assurance governance structure, with clear lines of Information Asset ownership and reporting with well-defined roles and responsibilities

2. Incident Management

- Ensure that identified information threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual information incidents are managed in accordance with NHS IG requirements.
- To ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the Organisation. These mechanisms should accommodate technical, operational or procedural improvements arising from lessons learnt.

3. Leadership

- Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience, provision of training and creation of information risk reporting structures.
- Advise the Board on the level of Information Risk Management performance within the Organisation, including potential cost reductions and process improvements arising etc.

4. Training

- Complete all required IG training relevant to the function of SIRO, including mandatory and strategic information risk management modules, annually as outlined in the Information Governance Training Plan 2015-2018.

Appendix B

Information Asset Owner (IAO) – Key Responsibilities

1. Policy and process

- Identify and document the scope and importance of all Information Assets they own, including purpose, justification, use and sharing/flows for each asset. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the Information Asset.
- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, regular review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks in line with the Trusts Information Risk Assurance Programme.
- Report to and provide support to the organisation’s SIRO, Senior Information Governance and Risk Officer and Risk Management processes to maintain their awareness of the risks to all Information Assets that are owned by the organisation and for the organisation’s overall risk reporting requirements and procedures.
- Ensure that staff and relevant others are aware of and comply with expected IG working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.
- Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets.

2. Incident Management

- Ensure that the organisation’s requirements for information incident identification, reporting, management and response apply to the Information Assets they own. This includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.

3. Leadership

- Foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the organisation’s policy.

4. Training

- Complete all required IG training relevant to the function of IAO, annually, as outlined in the Information Governance Training Plan 2015-2018.

Appendix C

Pennine Care NHS
NHS Foundation Trust

INFORMATION GOVERNANCE TRAINING PLAN 2015 – 2018

1. Requirements for Information Governance Training

The Information Governance Toolkit specifies uptake of a number of training modules to support certain requirements:

Requirements 112, 300 and 307 specify the following:

1.1 **Requirement No. 112 -** “Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained.”

“To ensure organisational compliance with the law and central guidelines relating to Information Governance (IG), staff must receive appropriate training. Therefore, IG training is ***mandatory*** *for all staff, (comparable to health and safety training) and staff IG training needs should be routinely assessed, monitored and adequately provided for.”*

This is also specified in the **NHS Operating Framework – Informatics Planning 2010/11** which provides guidance on the informatics components of local operating plans. National expectations for the NHS for delivery of national and local objectives are set out, building on existing investments to strengthen local information and data management. Under **‘Annex 1 National Expectations’** the section on sustaining robust information governance (IG)’ states that: *‘All staff should receive annual basic IG training appropriate to their role through the online NHS IG Training Tool.’*

In addition, confirmation of IG training being mandatory is documented in the **DoH Guidance for NHS Boards: Information Governance – August 2011** *“Appropriate annual information governance training (which may be via the on line training tool), is mandatory for all staff who have access to personal data and for all those in key roles.”*

1.2 **Requirement No. 300** – “The Information Governance (IG) agenda is supported by adequate information security skills, knowledge and experience which meet the organisation’s assessed needs.”

“Information security is a key element of the IG agenda. The information security assurance framework should be supported by adequate skills, knowledge and experience across the whole organisation. The levels of competency should be commensurate with the duties and responsibilities of particular posts or staff groups to provide an adequate level of assurance.”

1.3 Requirement No. 307 – “An effectively supported Senior Information Risk Owner (SIRO) takes ownership of the organisation’s information risk policy and information risk management strategy.”

“Organisations should ensure that appropriately senior individuals are allocated responsibility for owning information risk. In NHS organisations this role is referred to as the Senior Information Risk Owner (SIRO), who should be an Executive Director or other senior member of the Board (or equivalent), e.g. senior management committee. SIROs should be familiar with information risks and the organisation’s response to risk to ensure they can provide the necessary input and support to the Board and to the Accounting Officer.”

The SIRO is required to successfully complete strategic information risk management training at least annually.

Information Asset Owners (IAOs) must also be appropriately trained to carry out their roles.

2. Training Needs Analysis

Please note, the Trust Training Needs Analysis is subject to review during 2017/18 as new NHS tools become available. Please refer to the Information Governance Team / Records Management Team for the latest guidance re training beyond the annual mandatory module requirement.

2.1 The above requirement is already covered within the Trust’s Education, Training and Development Policy C05 (Appendix 1 of that Policy) and includes all staff groups within the Trust. There is additional training available to all staff, which can be arranged via the Information Governance / Records Management Teams.

2.2 New Staff

Information Governance basic training takes place at every induction via the workstation learning format. All staff (substantive, temporary and students) receive the corporate induction. Corporate induction runs 22 to 24 times per year.

Additionally, the Trust provides four further inductions for psychiatrists (training grades) and the Practice Education Facilitators provide two induction sessions for student nurses entering fieldwork practice within the Trust.

Students from other groups e.g. occupational therapists are prepared for fieldwork by the Higher Education bodies and, as such, may not receive the Information Governance information at induction. These students are, however, supervised by staff who will have undertaken the Information Governance training.

At corporate induction, staff are instructed to complete the mandatory on-line IG training within one month of starting their post.

2.3 Current staff

If the **Introduction to Information Governance** or the **Information Governance: the Beginner's Guide** have previously been completed and passed within the last 12 months, the requirement is to complete:

Information Governance: The Refresher Module – this must be completed every 12 months.

The importance of good clinical record keeping - Any staff using clinical records should also complete a training module every 3 years or undertake face to face training provided by the Records Manager(s).

NHS Information Risk Management for SIROs and IAOs - the SIRO must undertake this module every 12 months and it is recommended that Information Asset Owners, Information Asset Managers and relevant Information Asset Administrators also complete additional training as made available by the Trust, every 12months.

Managers are requested to recommend staff members to complete additional training where appropriate.

2.4 Staff with no direct access to a PC or without basic ICT skills

The Trust recognises that not all staff will have direct access to a PC or possess the basic ICT skills needed to undertake the required training via the on-line training tool. The Department of Health has confirmed that a combined approach (including e-learning and face-to-face training) would be acceptable to evidence the delivery of IG training for the IG Toolkit Requirement No.112.

If required, the Senior Information Risk and Governance Officer will develop a number of bespoke ad-hoc training sessions to be delivered throughout the Trust, where required. Staff undertaking the training in this way will be evaluated and, should they reach an acceptable level of understanding i.e. 80% pass, they will receive a certificate for their portfolio.

3. Accessing training via ESR e-learning

In addition to attendance at induction and annual mandatory update training sessions, all staff are required to complete a mandatory e-learning Information Governance module. It is a Department of Health requirement that at least 95% of all staff are trained on the required IG modules at any one time. All of the Trust's workforce (including all permanent staff and staff on temporary contracts of more that three months) must receive basic Information Governance training.

All staff should access the Mandatory IG training: *Introduction to Information Governance or Information Governance – The Refresher Module*, through the ESR e-learning gateway.

IG training is now included within the Core and Essential e-learning courses along with all other core e-learning.

All staff must register by clicking on the following link:

http://www.nwyhelearning.nhs.uk/elearning/northwest/penninecare

User guides and further information can be found under the OL&D E-learning site.

4. Reporting and Monitoring

Responsibility for monitoring the uptake of IG training will be managed by the Information Governance Assurance Group and performance levels are reported to Executive Directors and all IAOs at least quarterly.