East of England Ambulance Service NHS Trust

Information Governance Policy

Document Reference	POL009
Document Status	Approved
Version:	V8.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
Information Governance Requirements	September 2007	Information Governance Group
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
1.0	September 2007	Approved - IGC
1.1	March 2010	Reviewed by Clinical Quality Manager – submitted to IGG for comment
2.0	April 2010	Approved by Integrated Governance Committee
2.1	June 2012	Reviewed by IG Manager
2.1	July 2012	Recommended by IGG
3.0	July 2012	Approved at EMT
3.0	23rd February 2015	Review date extension agreed by IGG following approval by EMB
4.0	17 December 2015	Approved by Executive Leadership Board
5.0	4 August 2016	Approved by Executive Leadership Board
6.0	7 August 2017	Approved at Senior Leadership Board
6.1	22 May 2018	Approved at Information Governance Group
7.0	June 2018	Approved at Senior Leadership Board
7.1	March 2019	Approved at Information Governance Group
8.0	20 March 2019	Approved at Management Assurance Group

Document Reference	NHS Digital Data Security Protection Toolkit Directorate: Clinical Quality Directorate
Recommended at Date	Information Governance Group 12 March 2019
Approved at Date	Management Assurance Group 20 March 2019
Review date of approved document	2 years from date of approved document
Equality Impact Assessment	
Linked procedural documents	Records Management Policy Information Security Policy Data Protection Policy Internet Use Policy Email Use Policy Freedom of Information Policy Any other policies related to information governance
Dissemination requirements	All Trust staff
Part of Trust's publication scheme?	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Appendices

1. Introduction

The East of England Ambulance Service NHS Trust (EEAST) provides emergency and urgent care services, across 7,500 square miles and serving six million people. The Trust is a valuable public resource which is utilised to secure the best possible outcomes for patients. In doing so, it seeks to meet its vision and values, its NHS contract and to uphold the principles of the NHS Constitution. To provide these services to patients in the East of England the Trust recognises that information is a vital asset. Information is therefore of paramount importance in terms of the clinical management of patients, the financial management of the efficient use of resources to meet performance and quality standards and to meet public expectation. Appropriate and relevant strategies, policies, procedures and management accountability provide a robust governance framework to deliver the principles of information governance.

This information governance policy has been developed to give assurances that the Trust will handle all information in a confidential and secure manner and in accordance with relevant quality and legislation standards appropriate to operating a modern ambulance service.

EEAST will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Digital Data Security Protection toolkit and the new data protection legislation and accompanying guidance from the Information Commissioner's Office.

This policy should be read in conjunction with the Trust's Information Governance Strategy.

2. Principles of Information Governance

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust also recognises the need to share 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.

Equally important is the need to ensure high standards of data protection and confidentiality to safeguard personal/sensitive and commercially sensitive information. Underpinning this is the integrity need for electronic and paper information to be accurate, relevant, and available to those who need it.
Staff must ensure at all times that high standards of data quality, data protection, integrity, confidentiality and records management are met in compliance with the relevant legislation and NHS guidance.

From 25 May 2018 the main piece of legislation is the EU General Data Protection Regulation (GDPR). This is being complemented with domestic legislation, which will become the new data protection legislation. This will also apply to any organisation that processes information on behalf of the Trust, e.g. third party data processors. Under GDPR there are six principles to govern how person-identifiable information is processed:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.

This is further supported by the Caldicott Guardian principles, outlined in the 2016 Caldicott3 report.

3. Purpose

The purpose of this policy is to inform all Trust staff of their responsibility for ensuring that corporate, patient and personal information is safeguarded and used appropriately within the Trust. It is the responsibility of all staff to familiarise themselves with this policy and adhere to its information governance principles.

All aspects of handling personal and special categories of information are covered by this policy, including paper and electronic structured record systems and the transmission of information via mail, e-mail, fax and telephone.

Personal data is defined as Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data (formerly known as sensitive data) is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This policy covers all systems utilised by EEAST and any individual employed, in any capacity, by the Trust.

The aims of this Trust policy are to maximise the value of the Trust's assets by ensuring:

- Openness

- Legal Compliance
- Information Security
- Quality Assurance

3.1 Openness

Non-confidential information on the Trust and its services will be made available to the public through its public website.

The Trust will establish and maintain policies and its publication log to ensure compliance with the Freedom of Information Act 2000.

Patients will be able to exercise their right to access patient care record information relating to their own clinical care, through the Trust's release of information team.

3.2 Legal Compliance

The Trust regards all identifiable personal information relating to patients as confidential.

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 to ensure compliance with the current data protection legislation, Human Rights Act and 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, Protection of Children Act).

There must be a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The lawful basis must be determined and documented before processing. The Trust privacy notice should include the lawful basis for processing as well as the purposes of the processing. Processing of special category data requires both a lawful basis for general processing and an additional condition for processing.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

When processing special category data, you need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes

and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.3 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 and training.

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.

3.4 Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of records.

Managers are expected to take ownership of, and seek to improve, the quality of information within their departments. Wherever possible, information quality should be assured to 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.

4. Roles and Responsibilities

4.1 Trust Board

Ultimate responsibility for information governance in the Trust rests with the Trust Board who will ensure that the information governance strategy is implemented via this information governance policy and related policies.

4.2 Chief Executive

As the accountable officer for the Trust, the Chief Executive is responsible for meeting all statutory requirements and required to provide assurance that all information risks to the Trust are effectively identified, managed and mitigated. Details of Serious Incidents involving data loss or confidentiality breaches must be recorded on Datix and on the NHS Digital Serious Incident Reporting tool. All Serious information Incidents are reported in the annual quality account report.

4.3 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible to ensure all information risks are correctly identified, managed and that appropriate assurance mechanisms exist. This is achieved through ownership of the Information Asset Register and ensuring that risk assessment processes are completed and implemented by the Information Asset Owners. Business continuity plans will be reviewed by the SIRO to ensure that all information risks are linked to business continuity plan and are exercised on a regular basis. The SIRO will ensure that the Trust has systems in place that detail and monitor information flow mapping contained on the Information Asset Register, both internal and external. The Trust's Senior Information Risk Owner is the Executive Director for Strategy and Sustainability.

The SIRO is required to provide advice to the accountable officer (Chief Executive) on the content of the Trust's statement of internal control in regard to information risk and for bringing data protection issues for consideration to the Trust Board and act as advocate for information risk on the Trust Board.

4.4 Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Caldicott Guardian is responsible for providing advice within the Trust on the lawful and ethical processing of patient information and will represent and champion Information Governance requirements and issues at Board level. The Caldicott Guardian will ensure that confidentiality issues are reflected in the Trust's strategies, policies and procedures for staff. In addition the Caldicott Guardian will oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the Trust. The Medical Director has been appointed as the Trust's Caldicott Guardian and the Consultant Paramedic is recorded as the Deputy Caldicott Guardian.

4.5 Data Protection Officer

Has the leadership function for IG, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle person-identifiable information. The Data Protection Officer will be the first point of contact for any information governance related queries both internal and from external parties and will drive forward the information governance agenda. The Data Protection Officer will report any serious information governance concerns via the Caldicott Guardian and SIRO to the Chief Executive and will retain operational independence at all times.

4.6 Audit Committee

The Audit Committee will report to the Trust Board on the operation of the Trust's Information Governance Policy. The Committee will receive appropriate information via the Information Governance Group and will monitor compliance with all relevant legislation and this policy.

4.7 Information Governance Group

The Trust's Information Governance Group has responsibility for the formulation of Information Governance policies. This group has senior level representation from all appropriate departments within the Trust to ensure the Trust steers this agenda in line with current legislation. The Information Governance Group will receive reports on the Trust's compliance with the timescales laid out by the current data protection legislation from the Information Governance Manager and Human Resources Department. They will also monitor the types of requests received and the type of applicants making the requests.

The Information Governance Group will monitor the release of information from the Trust; feeding any recommendations for improvement to the Audit Committee and is reportable to the Audit Committee to provide assurance around Information Governance. The IGG will also approve central returns required by NHS Digital, specifically in reference to the Data Security Protection (DSP) Toolkit.

4.8 Compliance and Standards Lead

The Compliance and Standards Lead is responsible for overseeing the information governance systems and processes within the Trust, raising awareness of information governance issues, and ensuring that good information governance practices are adopted.

4.9 Information Governance Manager

The Information Governance Manager provides day-to-day operational support to the Compliance and Standards Lead and manages the information governance processes for the Trust. This role is responsible for organising and enforcing the Trust's approach to data protection. The Information Governance Manager will ensure that the Information Governance Work Plan is implemented and that a senior manager is nominated for each work area.

4.10 Trust Managers

Staff with areas of responsibility related to information governance is expected to have input to the Trust's information governance agenda, either by membership of the Information Governance Group, as responsible officers for DSP Toolkit requirements, or by ad-hoc input, as required. They should ensure that the working practices carried out within their department are in line with Trust policy and that all staff are adequately trained.

4.11 All staff (including temporary staff and volunteers)

All staff are responsible for ensuring that they adhere to this policy and implement best practice in relation to information governance wherever possible. They are responsible for raising incidents relating to information governance on the incident reporting system or via their line manager.

4.12 Consultation and Communication with Stakeholders

This policy is reviewed and approved by the Information Governance Group, which includes key information governance stakeholders from corporate and operational areas in the Trust.

5. Effective information governance management

5.1 Data Security Protection (DSP) Toolkit and internal audit

From April 2018, the Trust's IG compliance will be measured by a self-assessment process of compliance against the ten standards set out in the Data Security Protection Toolkit. This is and will be complemented by the annual internal audit and any recommendations made are monitored by the Audit Committee.

5.2 Care Quality Commission Oversight

CQC, as outlined in *Safe Data, Safe Care* (2016),[1] have powers to inspect the Trust's IG as part of its inspection round. To this end the Trust must ensure that robust IG practices are in place. CQC specifically requires that Medical Records are accurate, fit for purpose, held securely and held confidential.

5.3 Mandatory training and awareness

Fundamental to the ever-developing information governance agenda is the engagement and awareness of staff. This is currently driven by the requirement for 95% of staff to have completed information governance training (v.14.1 HSCIC IG Toolkit).

The Trust identifies that key staff or staff groups will require additional training, such as the SIRO, Caldicott Guardian and Data Protection Officer as well as specific staffing groups. This will be identified in the training needs analysis that has been shared with the People and Education Department.

5.4 Information Asset Management and Business Continuity

A core IG objective is that information assets and the use of information in them are identified and that the business importance of those assets is established.
Information assets are those that are central to the efficient running of the Trust and specific departments, e.g. patient, finance, stock control etc, essentially, it is information that is of value to the organisation and would be problematic if it were not accessible.
IAOs are usually senior members of staff who are the nominated owner for one or more of the Trust's identified information assets and it is their responsibility to record their information assets on the Trust's Information Asset Register; review these at least annually and undertake a Data Flow Mapping exercise. The Information Asset Register is overseen by the Trust's SIRO and identified risks will be recorded on the Trust's Risk Register. All data flows should have a documented legal basis and this should be recorded on the Information Asset Register.

5.5 Data Protection Impact Assessments

In line with the Information Commissioner guidance, a data protection impact assessment should be completed on any new or changing transfer of personal data. This could be the procurement of a new system or changes to how we use information in an existing asset.

These assessments must be completed by the nominated project leads with advice and support provided by the Information Governance Manager.

5.6 Confidentiality

Decisions about any disclosure of personal/sensitive information must be made on a case by case basis referring to the concepts laid down in this policy.

A duty of confidence arises when a person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is therefore:

- A legal obligation that is derived from case law – the Common Law Duty of Confidence
- A requirement established within professional codes of conduct – HCPC, MNC, GMC
- A clause within your contract of employment linked to internal procedures such as the disciplinary procedures.

Never give out information to persons who do not “need to know” in order to provide health care and treatment, or for any other reason.

All requests for patient identifiable information should be justified. This applies whether the request comes from within the Trust or from some outside organisation. Some requests may need to be agreed by the Trust’s Caldicott Guardian.

Every NHS Trust has a Caldicott Guardian. This is usually a senior manager who is also a doctor or a nurse. In the East of England Ambulance Trust the role of Caldicott Guardian is undertaken by the Medical Director. Their role is to protect patient confidentiality as far as possible. They should be contacted if you are in doubt about disclosure or if you are aware of poor practice within the Trust which may be putting patient confidentiality at risk.

5.7 Registration Authority

The Trust delegates the responsibility of the registration authority work stream to the information governance department alongside the Workforce Planning and Information team.

6. Development

6.1 Prioritisation of Work

The Policy is required for staff information and reference and to support the Trust’s wider Information Governance Framework.

6.2 Identification of Stakeholders

Primary stakeholders are the Caldicott Guardian, Executive Director for Strategy and Sustainability (as the Trust SIRO), Data Protection Officer Compliance and Standards Lead, Information Governance Manager and members of the Information Governance Group.

6.3 Responsibility for Development of the Document

The Policy has been developed by the Information Governance Manager, with review and approval by the Information Governance Group.

7. Use of Information within the Trust

The Trust is committed to proactively using the information we hold to improve patient care and for the service development, providing this is in line with the relevant legislation and current best practice guidance.

The Trust will ensure that non-confidential information is easily accessible to members of the public through the publication scheme under the Freedom of Information Act 2000 and that we are open and transparent with the information we hold.

8. Transfer of Information into and out of the Trust

The Information Governance Manager will ensure information flows into and outside of the Trust are appropriately recorded on Datix and monitored for review annually. Any risks associated with these information flows will be identified and recorded on the Trust's risk register.

These information flows will be completed in line with the Caldicott Guardian principles, contractual terms and the current data protection legislation.

Information Sharing Agreements are reviewed by the Caldicott Guardian and approved by the information governance group. All ISA's are stored centrally by the IG Manager on the Healthassure system.

9. Disclosure of information

The disclosure of any personal data outside of the points above will be processed under the Data Protection Policy and disclosure of corporate information will be dealt with under the Freedom of Information Policy.

9.1 Data Subject Rights

Data subjects have increased rights under the new data protection legislation:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

10. Incident and Risk Management

Any incidents related to information governance should be reported on the Trust's incident reporting system, DATIX. A decision will be taken whether it is necessary to report this as a Serious Incident under the Serious Incident Policy and/or to the Information Commissioner by the Serious Incident Panel and Information Governance Manager. The incident will also be processed through the NHS Digital Serious Incident reporting tool to support this decision. A serious breach of any information governance policy could result in action being taken under the Trust's Disciplinary Policy.

The Information Governance Manager will identify potential risks to the Trust from the incident investigation process and record these onto the Trust's Risk Register. These risks will be reviewed by the Information Governance Manager monthly and at the Information Governance Group on an annual basis.

11. Legal and Trust Related Policies

The Trust has a range of policies supporting the information governance agenda. Legal and professional guidance will be considered where appropriate by the Compliance and Standards Lead and/or the Information Governance Manager.

12. Information Governance Management

The Information Governance Group (IGG) is responsible for overseeing the Trust's information governance strategy, including:

- Developing and maintaining policies relevant to IG
- Developing standards and guidance relevant to IG
- Reviewing information sharing arrangements with other organisations
- Promoting awareness of IG issues

The Information Governance Group reports to the Audit Committee.

13. Training

Information Governance is included in the Trust induction training and as part of the annual mandatory update training for all staff and a full training needs analysis has been completed in relation to these aspects. Additional training can also be requested at the discretion of a manager, or by an individual wanting personal development.

The People Development and Education Department of the Trust, in conjunction with the Information Governance Manager, is responsible for designing an Information Governance training package. Uptake of training is monitored through the PDE Department.

Further guidance and information relating to IG issues will be distributed periodically via various media including bulletins and newsletters.

14. Equality Impact Assessment

An Equality Impact Assessment has been undertaken.

15. Dissemination and Implementation

15.1 Dissemination

This Policy will be disseminated to staff via the Trust intranet. Significant revisions and updates to the Policy will also be promoted in the staff bulletin.

15.2 Implementation

Awareness of the Policy and compliance with its requirements will be promoted via information governance training sessions, such as the induction programme for new Trust staff and annual refresher training for existing staff.

The IG Team will monitor staff compliance with the requirements of the Policy as part of their ongoing work, and take action to rectify any perceived weaknesses in compliance as necessary. Any weakness or areas of good practice will be shared with the Information Governance Group.

16. Process for Monitoring Compliance and Effectiveness

See Appendix A – Monitoring Table.

The security and integrity of the information processes within EEAST will be monitored for compliance by the Information Governance Group who will escalate any areas of concern to the Audit Committee.

17. Standards/Key Performance Indicators

The Key Performance Indicator for this Policy is satisfactory compliance with the requirements of the annual NHS Digital Data Security Protection Toolkit return.

18. References

- The Common Law Duty of Confidentiality
- Current data protection legislation (EU General Data Protection Regulations and UK data protection legislation)
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- The Human Rights Act 1998 (article 8);
- Computer Misuse Act 1990
- ISO 9000 Information Security Management
- The Crime and Disorder Act 1998 (section 115);
- Civil Contingencies Act 2000
- Protection of Children Act 2010
- Clinical Information Quality Assurance

- Corporate Information Quality Assurance
- Records Management: NHS Code of Practice
- NHS England Contract
- NHS Operating Framework
- Caldicott Guardian seven principles
- IG Toolkit
- Electronic Communications Act 2000
- A Paperless NHS: Electronic Health Records

Appendix A – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Information Governance Toolkit	Information Governance Team.	Progress reports from IG Team. Review of interim Toolkit scores. Review of independent internal audit reports.	Bi-monthly updates at IGG. Annual report to Board.	Formal written reports.	Review by Information Governance Group. Formal progress reports will be discussed and required actions and timescales agreed. Decisions of the Group will be formally recorded in minutes.	Information Governance Manager with support from the IG Team and designated IGG members.	Review of processes underpinning the IG Toolkit scores, to improve the Trust's overall IG framework and hence compliance with the requirements of the Toolkit.
Information Governance Risk Register	Information Governance Team. SIRO.	Progress reports from IG Team. Monitoring of the Trust Risk Register (4Risk).	Bi-monthly updates at IGG. Annual report to Board.	Summary reports from the 4Risk system.	Review by Information Governance Group. Ongoing monitoring by the Risk Manager. Formal progress reports will be discussed at IGG and required actions and timescales agreed. Decisions of the Group will be formally recorded in minutes.	Information Governance Manager Other risk leads deemed responsible for the area where the IG risk occurs.	Action taken to improve controls and mitigate any IG-related risks, reducing risk score.
Information Governance Awareness Training	Information Governance Team. Learning and Development. Unit	Training completion reports.	Monthly reports from LDU. Bi-monthly updates at IGG.	Formal written reports.	Review by Information Governance Group. Ongoing monitoring by the Learning and Development Manager. Formal progress reports will be discussed at IGG and required actions and timescales agreed. Decisions of the Group will be formally recorded in minutes.	Information Governance Manager Learning and Development Manager.	Action taken to ensure that all staff have completed either information governance induction training or annual refresher training.

Appendix B
Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference: POL	Document Title: IG Policy
Assessment Date: 22 June 2016	Document Type: Policy
Responsible Director: Director of Finance	Lead Manager: Information Governance Manager
Conclusion of Equality Impact Assessment: The Policy is E&D neutral and has no impact, positive or negative.	
Recommendations for Action Plan: None.	
Risks Identified: None.	
Approved by a member of the executive team:	
YES	**NO**
Name: Kevin Smith	Position: Director of Finance
Signature:	Date: 22 June 2016

This whole document should be stored with the master document.