East of England Ambulance Service NHS Trust

Information Governance Assurance Framework

Document Reference	POL008
Document Status	Approved
Version:	V4.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author**
IG Toolkit Requirements	November 2010	IG Manager
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
V0.1	November 2010	First draft written
V1.0	December 2010	Presented at IGG
V1.3	October 2011	Updated to ensure consistency with CfH IG Toolkit requirements
V1.3	January 2012	Presented at IGG
V1.4	August 2012	Document revised; format updated to comply with Policy on Procedural Documents
V1.5	December 2014	Review date extension approved by
V1.5	23rd February 2015	Review date extension agreed by IGG following approval by EMB
V1.5	4th December 2015	Approved by Information Governance Group

V2.0	17th December 2015	Approved by Executive Leadership Board
V3.0	4 August 2016	Approved Executive Leadership Board
V3.1	11 July 2017	Reviewed – Change to Trust SIRO
V4.0	7 August 2017	Approved Senior Leadership Board

Document Reference	IG Toolkit – Information Governance Framework Requirement **Directorate:** Clinical Quality Directorate
Recommended at Date	Information Governance Group 25 July 2017
Approved at Date	Executive Leadership Board 7 August 2017
Review date of approved document	7 August 2019
Equality Impact Assessment	Completed
Linked procedural documents	Information Governance Policy Information Governance Strategy Risk management Procedure Confidentiality Code of Conduct Safe Haven Policy
Dissemination requirements	All Trust staff
Checklist completed?	Yes
Part of Trust's publication scheme?	No

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. Background

The purpose of the Information Governance Assurance Framework is to formally establish the East of England Ambulance Services position in regard to way it handles information governance and how it provides assurance through operating within an Information Governance Assurance Framework.

- **Information Governance** describes the holistic approach to managing information by implementing processes, roles, controls and metrics that treat information as a valuable asset. It describes the legal framework and any best practice used to regulate the manner in which information is managed. In the Trust this involves a number of departmental teams working within the Finance, Operations, Human Resources, Information Management and Technology, Business and Clinical Quality Directorates.
- **Information Assurance** describes the confidence in the processes of information risk management specifically. It is the practice of managing the appropriate levels of availability, integrity and confidentiality – whether information is in storage, processing or transit, and if it is threatened by malice or accidental error, fraud, privacy violation, service interruption, theft or disaster.

Operating across a wide geographically area and using a number of electronic and paper systems to manage personal and commercial data can lead to creating potential information risks to the operation of the Trust. The intent here is to consolidate the Trust's Information Governance and Assurance arrangements and risk mitigation measures into one central document. This Framework therefore details the people, places and processes which are in place to ensure that the appropriate staff have access to the appropriate information, at the appropriate time. The need for the Trust to continue to enhance people's confidence in the safety of their data in the context of the increased risk that digital technologies can pose is critical. Public confidence in the Trust's ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe and secure at all times. This will require the Trust to continue to work hard to mitigate any potential risks created through implementing future digitalised systems as the Trust works towards a paperless NHS by 2020. The Trust relies on high quality information not only for its staff but for making its services to patients more responsive, safer, more effective and more efficient. It is important for staff to understand their own responsibility for recording information to a consistently high standard and for keeping it safe, secure and confidential. To support the Trust to achieve this aim the Trust must work within its Information Governance Assurance Framework to ensure all information is handled fairly and lawfully at all times.

Information is an important asset to the Trust and Information Governance (IG) is a corporate-wide agenda which underpins both clinical and corporate governance. It cannot be successful if it is seen in isolation from the Trust's wider integrated governance agenda.

2. Introduction

To improve the level of risk associated with the use of information technology the Trust is required to work within the parameters of an information governance assurance framework. Information governance is an umbrella term used within the NHS to inform all stakeholders that there is a set of standards, processes and procedures which the Trust is required to achieve to remain compliant. The level of compliance attained will provide the level of assurance to the Executive Leadership Board and to the Trust Board that all information is kept confidential and secure and that all records held by the Trust meet the NHS Code of Practice which is based on current legal requirements and professional best practice. It

encompasses legal requirements, central guidance and best practice in information handling and includes:

- The Common Law Duty of Confidentiality
  Data Protection Act 1998
- 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
- The Children Act 1989
- The Children Act 2004
- 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

3. Purpose

This document gives a background to the information governance agenda, and sets out an overarching framework for the implementation of an effective information governance programme at the East of England Ambulance Service NHS Trust (EEAST).

This Framework should be read in conjunction with the Information Governance Strategy and Information Governance Policy, which outline the Trust's Information Governance agenda at strategic and operational levels. Other related Trust policies are the Confidentiality Code of Conduct, Freedom of Information Policy, Records Management Policy, Risk Management Policy, Release of Information Policy, Information Security Policy and Clinical Quality Strategy.

4. Information Governance Roles and Responsibilities

4.1 Trust Board

The Trust Board has ultimate responsibility for ensuring that the Information Governance Assurance Framework provides a structure in which the Trust operates and handles all information fairly and lawfully.

4.2 Chief Executive

As the accountable officer for the Trust, the Chief Executive is required to provide assurance that all risks to the Trust (including information risks) are effectively identified, managed and mitigated. Details of Serious Untoward Incidents involving data loss or confidentiality breaches must also be detailed in the annual 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 in place an up to date information mapping diagram which details the Trust's Personal Data processing activities In and Out of the Trust. The Trust's Senior Information Risk Owner is the Executive Director for Strategy and Sustainability.

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. The Trust's Caldicott Guardian is the Medical Director

4.5 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 throughout the Trust.

4.6 Information Governance Manager

The Information Governance Manager provides day-to-day operational support to the Compliance and Standards Lead. The Information Governance Manager will review the Information Governance Assurance Framework and present the review and updates to the Information Governance Group for approval. The update IGAF will then be submitted to the Executive Leadership Board for approval and sign off. Once signed off the IGAF will be uploaded onto the Trust's public website.

4.7 Information Asset Owners

An Information Asset Owner (IAO) should be designated for each of the Trust's major information assets (both electronic and manual), as identified on the Trust's Information Asset Register. Information Asset Owners must understand their area of the Trust's business and be able to demonstrate detailed knowledge of how information is used as a resource in their area. Information Asset Owners are responsible for the ongoing maintenance and update of the Trust's Information Asset Register, and must provide assurance to the SIRO that information risks within their respective directorates and departments have been identified and recorded, with controls in place to mitigate those risks. Residual risks should be recorded on the Trust's Risk Register, as appropriate. The IAO must develop Business Continuity Plans and link them to their information risks. Plans should be tested on a regular basis.

4.8 Information Asset Administrators

Information Asset Owners have the discretion to appoint Information Asset Administrators (IAA) to effectively manage the information assets under their control, given operational requirements and budgetary constraints.

Information Asset Administrators will provide day-to-day support to the Information Asset Owners. Their duties will include ensuring that information assets are accurate and secure, and that best information governance practices (as outlined in the Trust Information Governance Policy and Strategy) are followed.

4.9 All Trust Staff

All Line managers are responsible for ensuring that they and their staff are supported in their information assurance responsibilities. Staff at all levels in the Trust must ensure that they are aware of their obligations with regard to maintaining information security and patient confidentiality, and follow established best practice for information handling at all times.

4.10 Consultation and Communication with Stakeholders

This Framework is reviewed and approved by the Information Governance Group, which includes key information governance stakeholders from all directorates within the Trust.

5. Information Governance Toolkit (IGT)

The Information Governance Toolkit is an online assessment tool which is managed by the Health and Social Care Information Centre (HSCIC). The HSCIC has changed its name to NHS Digital July 2016. NHS Digital will be launching a new system in 2018 to reflect the recommendations in the National Data Guardian's Review of Data Security, Consent and Opt-outs report.

The IG Toolkit draws together legal requirements and the general condition requirements detailed in the Trust's NHS England Contract. It presents them as a set of specific information governance requirements with which the Trust is expected to comply. The requirement headings include;

- Information Governance
- Management
- Confidentiality and Data Protection Assurance,
- Information Security Assurance,
- Clinical Information Assurance and
- Corporate Information Assurance.

The Trust as a healthcare service provider is subject to a three stage reporting process in which it must submit IG evidence against the 35 IG Toolkit requirements relevant to the Ambulance Service on the following dates:

- 31 July 2017 Baseline Assessment
- 31 October 2017 Performance Update
- 31 March 2018 Final Submission

All requirements must achieve a level 2 to be deemed satisfactory.

6. Information Governance Framework

6.1 Objectives of Information Governance within the Trust

The Trust's Information Governance Framework (including the associated IG Strategy and IG Policy) is designed to ensure that the primary objectives of information governance (as defined by the HSCIC (NHS Digital) are achieved, i.e.:

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential, at all times.
- The integrity of information will be maintained and monitored to ensure that it is up-to-date, reliable and of satisfactory quality for its intended use.
- Information required for operational purposes will be kept secure and only made available to appropriate and authorised staff. Hardware must be encrypted with password codes.
- In managing information risk the Trust will comply with all relevant legislation. The Data Protection Act 1998 imposes statutory obligations on the Trust as it processes a high level of personal data. The DPA makes it clear that the Trust is legally responsible for ensuring that the personal data it creates, collects, stores, uses and handles must be protected in accordance with the requirements of the DPA. Supporting legislation is listed in section 2 above. The Trust will monitored and review its legal processes via the Information Governance Group.
- All staff will have access to appropriate training and education to ensure they understand their professional and legal responsibilities for secure information handling. Staff should refer to their employment contracts, job descriptions and professional codes of conduct to ensure the security and confidentiality of patient information.
- An Information Risk Management Strategy will be utilised to establish ownership of the Trust's information assets and the SIRO will ensure that associated risks are mitigated.

6.2 Information Governance Education, Training and Development

Structured training is essential for the development and improvement of staff's knowledge and skills regarding Information Governance. Effective information governance training must extend beyond basic confidentiality and security awareness. In order to develop and follow best standards of practice, staff need to understand the value of information and their responsibility for it. Knowledge should include data quality, information security, records management, confidentiality, legal duty, Data protection Act 1998 and access rights, and the rights of patients with regard to privacy and the release of their personal and/or sensitive personal data. All staff must receive introductory IG awareness training as part of the corporate induction programme. Staff are also required to complete mandatory modules via the online NHS Information Governance Training Tool within three months of joining the Trust. Refresher training in IG should be undertaken on an annual basis thereafter.

Information Asset Owners and Information Asset Administrators should satisfactorily complete information governance training via the online training tool prior to commencing their information management duties. Satisfactory completion of IG training by staff will be monitored via the learning and development unit and a report detailing attendance and the percentage of staff that have completed the training will be presented to the Information Governance Group on a bi-monthly basis.

The Information Governance Manager will be responsible for the development and delivery of the IG Training Strategy, in conjunction with the Learning Development Unit.

The Information Governance Manager will ensure that there is an adequate level of information governance awareness within the Trust, and will periodically arrange promotional campaigns. Staff will also be made aware of significant national information governance developments via articles in in-house publications, the intranet, awareness training sessions and briefings. Information governance reference materials (such as policies and procedures) will be published on the Trust intranet.

6.3 Information Risk Assessment and Management

A Trust Information Risk Management Policy is in place. This outlines the Trust's approach to information risk management, the information risk management structure and process (including assessment and incident reporting), and the contractual obligations of third parties with respect to information risk.

An Information Asset Register is used by the Trust to record all the Trust's information assets. The designated Information Asset Owners (IAOs) will be responsible for ensuring that the register remains up-to-date.

The Trust's risk management programme should include the ongoing review and assessment of risks associated with information assets, as identified and recorded on the Information Asset Register. Significant information risks which cannot be mitigated should be included on the Trust's corporate risk register and acknowledged at Board level.

All Trust staff should be made aware of the procedures for reporting actual or suspected information governance incidents, such as data loss or unauthorised disclosure. Event identification and reporting should be a core element of information governance induction training, annual refresher training and ad-hoc training (where applicable). Training should include the use of the Datix system for incident recording.

The SIRO (in conjunction with the relevant IAOs) must ensure that reported information incidents are investigated. Resulting reports and recommendations should be presented to the IGG and Trust Board.

Third party contractors who have access to Trust information must be made aware of the importance of reporting perceived or actual events, in line with the terms and conditions of service provision.

6.4 Information Governance Group

The Information Governance Group (IGG) has been established to:

- Co-ordinate information governance strategies and policies across the Trust.
- Ensure consistent and high standards of record keeping and information handling in accordance with statutory and legal requirements
- Support the provision of high quality care by promoting the effective and appropriate use of patient identifiable information.
- Foster a greater awareness and ownership of information governance throughout the organisation.
- Monitor ongoing compliance with the requirements of the HSCIC (NHS Digital) Information Governance Toolkit.
- Review proposed information sharing agreements with other Trust bodies and external organisations.
- Approve minutes, etc. produced by the Information Governance Operational Working Group.

6.5 Audit Committee

The IGG will report to the Audit Committee, which is a sub-committee of the Board. The Director of Finance is the link between the Information Governance Group and the Audit Committee. The IGG will provide regular updates to the Audit Committee. These will include any important decisions made, progress with ongoing Information Governance work, identified information risks, and related strategies and policies for approval. An annual information governance report will also be produced for the Trust, which will be presented to the Audit Committee who will update the Trust Board.

6.6 Information Governance Operational Working Group

The Operational Working Group is a sub-group of the Information Governance Strategy Group, and is accountable to it. Its purpose is to:

- Co-ordinate and monitor activities to embed good information governance practice across the Trust at an operational level.
- Facilitate the completion of the CfH Information Governance Toolkit to ensure that a) the Trust meets at least minimum compliance levels by the final submission date, and b) independent audit requirements are met.
- Escalate any identified risks of non-compliance with information governance requirements to the IGG.

7. Equality Impact Assessment

An Equality Impact Assessment has been undertaken. See Appendix D.

8. Dissemination and Implementation

8.1 Dissemination

This Framework will be disseminated to staff via the Trust intranet.

8.2 Implementation

Awareness of the Framework 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 Framework as part of their ongoing work, and take action to rectify any perceived weaknesses in compliance as necessary.

9. Process for Monitoring Compliance and Effectiveness

See Appendix C – 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 Performance and Finance Committee.

10. Standards/Key Performance Indicators

The Key Performance Indicator for this Framework is satisfactory compliance with the requirements of the annual Information Governance Toolkit return.

11. References

- The Common Law Duty of Confidentiality
- Data Protection Act 1998
- 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
- The Children Act 1989
- The Children Act 2004
- 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

12. Associated Documents

Information Governance Policy
Information Governance Strategy
Risk Management Procedure
Contract of Employment
Confidentiality Code of Conduct
Safe Haven Procedure

Appendices

A	Information Governance Group Terms of Reference
B	IG Operational Working Group Terms of Reference
C	Checklist
D	Monitoring Table
E	Equality Impact Assessment

Appendix A – Information Governance Group

Terms of Reference

1. Purpose

The Information Governance Group (IGG) has been established to co-ordinate information governance strategies and policies across the Trust, and to ensure consistent and high standards of record-keeping and information handling in accordance with statutory and legal requirements. It will support the provision of high quality care by promoting the effective and appropriate use of patient identifiable information, and assist in delivering one of the Trust's strategic objectives, i.e. to deliver safe, high quality effective services, and achieve good governance.

2. Constitution

The ultimate responsibility for the IGG lies with the Trust Board, which has delegated authority to the Executive Leadership Board to discharge its duties in this respect. The IGG is also accountable to the Audit committee, which is a sub-committee of the Trust Board and chaired by a non-executive director, who will provide assurances to the Board that the duties of the IGG have been discharged appropriately.

3. Membership

Head of Clinical Quality **(Chair)**
Compliance and Standards Lead **(Vice Chair)**
Senior Information Risk Owner – Executive Director for Strategy and Sustainability
Caldicott Guardian – Medical Director
Head of Clinical Quality
Consultant Paramedic
Locality Directors or nominated representative
Regional Head of Emergency Operations Centres
Head of Patient Transport Services or nominated representative
Head of Information Management and Technology
Head of Human Resources
Head of Primary Care
Head of Procurement
IM&T Security and Resilience Manager
IM&T Programme Manager
Research Manager
Learning and Development Manager
Information Governance Manager
Registration Authority agent/s
Clinical Records/Freedom of Information Manager
Corporate Records/Freedom of Information Manager

The above list represents core membership; other persons may be required to attend for specific agenda items. Any member unable to attend should ensure an adequately prepared

representative attends in their place. The quorum will be five members plus the Chair or Vice-Chair.

4. Frequency

The IG Strategy Group will meet bi-monthly.

5. Relationships

The Information Governance Group will report to the Audit Committee. It will provide regular updates, exception reports, strategies and policies for approval. An annual information governance report will be produced for the Trust each year. This will be derived from the achievements of the Information Governance Work and Improvement Plan (which will cover key areas of risk relating to information governance activities) and the Information Governance Toolkit submissions. This annual report will be presented to the Trust Board.

The Information Governance Group will act as a Strategic Group. A separate IGG Operational Working Group will be established, and this will report into the main Information Governance Group.

6. Duties

Information Governance

- To oversee the implementation of information governance activity within the Trust, including freedom of information, data protection, information quality assurance, health records, data quality, the Confidentiality Code of Practice, information security and information governance management.

- To work with the Caldicott Guardian to ensure patient-identifiable information is kept confidential and to monitor the procedures in place for the release of information to ensure compliance with the law and guidance.

- To be responsible for documenting confidential audit procedures and monitoring the outcome of these audits and the effectiveness of the procedures.

- To ensure that the Trust undertakes regular audits of the information governance processes in place, to demonstrate that improvements made comply with the information governance toolkit standards.

- To ensure staff have access to appropriate and up to date guidance on keeping personal information secure, on respecting the confidentiality of service users and on the duty to share information for care purposes.

- To approve an Information Governance Work and Improvement Plan, secure the necessary implementation resources, and monitor and report progress made against the plan. Where exceptions arise in the delivery of the plan these will be reported to the Executive Leadership Board so that issues can be resolved and any impact on the delivery of the Trust's strategic objectives can be reduced.

- To provide the focus for the direction, development, promotion and monitoring of information governance.

- To receive review or risk reports from the Information Asset Owners on an ad hoc basis and approve any recommendations.

- To produce a strategy covering general and long-term issues which guide the values, behaviour and arrangements necessary to manage information governance to optimum levels, having regard to cost, safety and quality of service provision.

- To continue to identify all purposes for which confidential personal information is required and shared and to determine the legal basis for such sharing or use.

- To receive and consider incident reports (including serious untoward incidents where there has been a breach of confidentiality and security), and where appropriate monitor the recommendations and actions taken to prevent similar adverse events reoccurring.

- To review the Trust's Information Governance Risk Register on an annual basis.

- To maintain links with the People Development and Education Department and training departments to ensure that all staff receive appropriate training and development in information governance, including Caldicott principles, confidentiality, data protection, information security and freedom of information.

- To establish communication channels to promote sound information governance principles and effective working arrangements with key stakeholders, including our staff, patients, carers and relatives.

- To ensure operational arrangements exist to allow staff to support and protect patients' privacy and confidentiality, and that staff are aware of their professional responsibilities to treat all patient information confidentially.

- To provide a focal point for the resolution of information governance issues and to ensure that the views of staff, patients, carers and relatives are included in the development of information governance arrangements within the Trust. To be responsible for ensuring that any new or proposed changes to organisational processes or information assets are identified.

- To approve and monitor the completion of Privacy Impact Assessments (PIAs) where appropriate.

- To regularly monitor the effectiveness of these Terms of Reference. Where monitoring has identified deficiencies, recommendations and actions must be made immediately to effect and implement changes accordingly.

Records Management

- To facilitate the continuity of care for our patients by the effective and efficient transmission of information between healthcare staff and monitor the healthcare records to ensure that the overall objectives of the organisation are met and that the Trust complies with best practice guidance and legislation.

- To identify and understand all categories of corporate records, ensure secure management and transfer of corporate records and monitor working practices to verify accuracy, accessibility, integrity and validity of corporate records.

- Be responsible for approving all policies and procedures relating to records management, ensuring staff are aware of the relevant documents and implementing regular monitoring standards, including an audit programme. This monitoring should be reported to the Executive Leadership Board on an annual basis.

7. REPORTING TO AUDIT COMMITTEE

Important decisions, identified risks, and meeting notes from the Information Governance Group will be presented at the Audit Committee.

Appendix B – Information Governance Working Group

Terms of Reference

1. Purpose

The Information Governance Working Group is a sub-group of the Trust Information Governance Group (IGG). Its purpose is to:

- co-ordinate and monitor activities to embed good information governance practice across the Trust at an operational level;
- facilitate the completion of the Information Governance Toolkit to ensure that a) the Trust meets at least minimum compliance levels by the final submission date, and b) independent audit requirements are met, and
- Escalate any identified risks of non-compliance with information governance requirements to the Information Governance Group.

2. Relationships

The Information Governance Working Group is accountable to the IGG Group which reports to the Audit Committee.

3. Membership

- Compliance and Standards Lead (Chair)
- Information Governance Manager (Vice Chair)
- IMT Security Manager
- FOI Officer / Clinical Records Manager
- FOI Officer /Corporate Records Manager
- Clinical Audit Manager
- Workforce Planning & Information Manager

- Other Trust Officers with assigned responsibility for Toolkit standards
- Other persons as required for specific agenda items.

4. Frequency and Attendance

The Information Governance Working Group will meet monthly always ensuring that it meets prior to the next scheduled IGG.

If core Group members are unavailable, then a deputy should be assigned to attend in their absence.

5. Authority

The group has no executive decision powers. It shall be directly accountable to the IGG and will provide a summary report of the proceedings of each meeting at the next scheduled IGG meeting. The group is authorised by the IGG to approve and ratify documents that support Trust Strategies and policies. The IGG delegate authority to the group to co-opt other persons/managers as required for specific agenda items and to gain independent professional advice when managing complex IG issues.

6. Duties

The subject matter for the meetings will be wide ranging and varied. In particular the group will review and create relevant IG policies and procedures, examine, co-ordinate and monitor IG compliance. It will support the evidence gathering for the quarterly IG Toolkit submissions and monitor progress against each toolkit requirement. It will allocate tasks on the work plan to improve the IG arrangements within the Trust.

7. Review

The Terms of Reference and membership of the Operational Working Group will be reviewed bi-annually, unless prompted by operational or legislative requirements.

Appendix C – Template for the Checklist for the Development or Review and Approval of Procedural Document

This should be completed and attached to any procedural document when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	Y	Framework for IG programme at EEAST.
2.	**Definitions**		
	Have all key terms been clearly defined?	Y	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	Y	
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	N	Pending
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	Y	
6.	**References/Associated Documents**		
	Are key references cited?	Y	
	Are linked documents identified where appropriate?	Y	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	Y	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	N/A	Dissemination via intranet.
	Does the plan include the necessary training/support to ensure compliance?	N/A	Covered as part of ongoing staff IG training.
8.	**Review Date**		
	Is the review date identified?	Y	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name	Gail Butler	Date	8th November 2012
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name	Not Applicable	Date	--
Please attach to the procedural document and forward to the relevant committee for approval			

Appendix D – 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 E – Equality Impact Assessment: Executive Summary

Executive Summary Page for Equality Impact Assessment:	
Document Reference: Version 4.0	Document Title: IG Assurance Framework
Assessment Date: 13th June 2016	Document Type: Framework
Responsible Director: Director of Finance (IGG Executive Member)	Lead Manager: Compliance and Standards Lead
Conclusion of Equality Impact Assessment: The Framework 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: - by email -	Date: 22nd June 2016
This whole document should be stored with the master document.	