NHS

Ashford and St. Peter's Hospitals
NHS Foundation Trust

Information Governance (IG) Policy

Author: Jane Townsend – Information Governance Manager

Executive Lead: Simon Marshall – Director of Finance

Status:	Approval date:	November 2021
	Ratified by:	Information Governance Steering Group
	Review date:	November 2022

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	Nov 13	Policy redraft	Mark Gubby, Information Governance Manager
2	Nov 14	Minor updates throughout; Reporting line to Audit Committee	Mark Gubby, Information Governance Manager
3	Jun 15	Minor updates throughout; Review date aligned to meet annual work programme	Mark Gubby, Information Governance Manager
4	Jun 16	Change to Information Governance Lead in line with new management structure	Jane Townsend, Information Governance Manager
5	Nov 2017	Addition of the DPO role	Jonathan Spinks, IT Programme Manager & Interim IG Lead
6	Sep 2020	General review	Jane Townsend, Information Governance Manager
7	July 2021	Rewrite of previous policy – draft shared for review at IGSG	J Townsend

For more information on the status of this document, please contact:	
Policy Author	Jane Townsend - Information Governance Manager
Department/Directorate	Digital Services
Date of issue	November 2021
Review due	November 2022
Ratified by	The SIRO, on behalf of the Information Governance Steering Group
Audience	All staff employed by ASPH Trust, Non-Executive Directors and Contractors.

Executive summary

1. How and why information needs to be managed and protected.
2. The structure of authority around the Trust’s information, who owns it and how we are all responsible for safeguarding it.
3. Required training for Information Governance compliance.
4. This Policy applies to:

- all those employed by the Trust who have access to information, including temporary staff, contractors and agency staff;
- all those engaged in duties for the Trust under a letter of authority, honorary contract or work experience programme;
- volunteers and all third parties such as contractors, researchers, students or visitors.

Hereafter, all the above are collectively referred to as ‘Employees’

Contents

SECTION **Page**

Appendices

1. Introduction

ASPH Trust (hereby referred to as ‘the Trust’) depends on the use and flow of information and data in order to deliver patient care and to meet its mandate. The confidentiality, availability and integrity of all information held and used by, or on behalf of, the Trust must therefore be assured. This requires robust Information Governance in order to:

- support clinical delivery, service planning and performance;
- enable the effective management of services and resources;
- ensure that all types of information in all formats are sourced, held and used appropriately, securely and legally;
- protect privacy and confidentiality;
- ensure the effective application of information security standards and behaviours throughout the Trust through a defined set of accountabilities;
- maintain public Trust.

This Policy describes the accountability framework for handling information in a confidential and secure manner to the appropriate professional and quality standards required of a modern health service. It brings together independent yet associated requirements and standards of practice, including people, policies, processes and technology.

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Ensuring data quality through the use of accurate, timely and relevant information is essential to deliver the highest quality health care. As such, it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to use information appropriately and actively in decision-making processes.

2. Scope

This Policy applies to all information obtained and processed within the Trust held electronically, in manual paper-based filing systems, and in other formats, relating (but not limited to):

- patient / client / service user information;
- Employee and personal information;
- organisational, business and operational information;
- clinical, research, audit and reporting information;
- commercial and contract details.

3. Purpose

This Policy provides the over-arching framework within which all information security issues shall be conducted and managed.

The purpose of this Information Governance Policy is to protect all information assets to a consistently high standard including manual and electronic records, both patient and corporate information, and to define a clear set of accountabilities in ensuring that protection. By promoting a culture of good practice around the processing of information at all levels, this Policy aims to ensure that all information held by or on behalf of the Trust is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically;
- shared and disclosed appropriately and lawfully;
- protected against unauthorised access.

4. Explanation of Terms Used

Term	Meaning / Application
SHALL	This term is used to state a **mandatory** requirement of this Policy
SHOULD	This term is used to state a **recommended** requirement of this Policy
MAY	This term is used to state an **operational** requirement of this Policy

The term Information Governance describes the structures, policies and practices used to ensure the confidentiality and security of the clinical records of patients/service users, employment records relating to Employees and Trust corporate business.

“Information” includes information in any medium, including paper records and electronic data, clinical records, letters, emails, CDs, DVDs, CCTV, X-rays, patient administration systems (PAS etc.), corporate information including Employees records, financial records, and estates and facilities records.

This includes the equipment that gathers or stores the above e.g. computers (networks, desktops), laptops, smart phones, paper records stores.

5. Duties and responsibilities

The Board

The NHS Chief Executive has made it clear that the ultimate responsibility for Information Governance, including data security and protection, rests with each Board of Directors. This Board shall therefore ensure that:

- Information Governance is explicitly referenced within the Trust's Statement of Internal Controls;
- there is always one person with overall responsibility for the protection of personal data;
- a Declaration of Maturity is produced against the criteria set out in the DSPT;
- the Annual Report of the Trust includes a Statement of Maturity as relates to Information Governance and Cyber Security;
- contractual arrangements with independent sector NHS providers contain strengthened Information Governance requirements;
- adequate training and support are provided to the individuals fulfilling the operational Information Governance roles and tasks set out in this Policy, and access is provided to further guidance and support;
- clear lines of reporting and supervision are established for compliance with personal data protection;
- regular checks are undertaken to monitor and assess the processing of personal data.

The Board is also responsible for setting the Trust's Risk Appetite regarding information security.

Senior Information Risk Owner (SIRO)

The Trust shall appoint an Executive member of the Board as the Senior Information Risk Owner (SIRO) and issue them with a Letter of Delegation.

The SIRO is accountable for information risk within the Trust and advises the Board on the effectiveness of Information Risk Management across the organisation, including the logging and monitoring of key information risks on the corporate Risk Register.

The SIRO shall:

- be accountable for the management and protection of all Information Assets;
- take overall ownership of Information Risk Management;
- provide a focal point for managing information risks and incidents;
- lead on Business Continuity in the context of Information Risk;
- act as champion for Information Risk on the Board;
- advise the Board on the effectiveness of Information Risk Management across the Trust;
- provide written advice to the Chief Executive Officer (CEO) regarding content to be included in the Declaration of Maturity for the Trust's self-assessment against the DSPT;
- ensure that Information Risk Assessments and management processes are embedded within the Trust;

- lead and foster a culture for protecting and using information and data;
- lead communications on Information Governance and Security throughout the organisation;
- approve and appoint Information Asset Owners (IAOs) and ensure each has a Letter of Delegation and appropriate Terms of Reference.
- The SIRO will chair and lead the Information Governance Steering Group (IGSG).

The SIRO shall work in liaison with all fellow board members and (if not a board member) the Chief Clinical Information Officer whose main focus is the integrity of systems and infrastructure.

Information Asset Owners

IAOs are senior/responsible individuals involved in running the Trust's clinical and corporate areas and who are the nominated owners of one or more identified information assets. The role of the IAO is to:

- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset;
- know who has access to the asset (whether system, portable technology, or information) and why, and ensure access is monitored and compliant with Policy;
- understand and address risks to the asset;
- foster a culture that values, protects and uses information for the benefit of patients, Employees and the Trust as whole;
- provide assurance to the SIRO on the security and use of information assets;
- advise the SIRO regarding Business Critical Information Assets in keeping with the Business Continuity and Disaster Recovery plans and the Information Security Policy.

These responsibilities shall be conferred in a Letter of Delegation from the SIRO who retains ultimate accountability for information handling across the Trust.

Information Governance Manager

The Trust shall appoint an Information Governance (IG) Lead to support the SIRO in ensuring the day-to-day operational effectiveness of information security policies including their management, accountability, compliance and assurance. This role will ensure that all service user, patient, Employee and corporate information within the Trust is created, maintained, transferred, reviewed and disposed of in a safe and secure manner.

The main responsibilities of this role include:

- ensuring that there is top-level awareness and support for Information Governance (IG) resourcing and implementation of improvements;
- formulating, establishing and promoting IG policies;
- establishing working groups, as directed by the SIRO;

- liaising with and providing guidance to IAOs in the fulfilment of their IG and DSP duties, as directed by the SIRO;
- coordinating the activities and progress initiatives of IAOs;
- ensuring that annual assessments using the DSPT and audits of IG policies and arrangements are carried out, documented and reported, in line with the requirements of the NHS Standard Contract;
- ensuring that annual assessments and improvement plans are prepared for approval by senior management in a timely manner;
- ensuring that the approach to information handling is communicated to all Employees and made available to the public regarding the safe sharing of personal confidential data;
- developing and delivering IG training to all Employees;
- leading or liaising with other committees, working groups and programme boards in order to promote and integrate IG and DSP standards, as directed by the SIRO;
- monitoring information handling activities to ensure compliance with established legislation and UK government, including NHS, guidance;
- providing assurance regarding the effective implementation of IG and DSP;
- monitoring potential and actual security breaches with appropriate expert security resource.

Caldicott Guardian

The Caldicott Guardian is an advisory role and acts as the “conscience” of an organisation, actively supporting work to facilitate and enable information sharing, and advising on options for lawful and ethical processing of information as required. The Caldicott Guardian reflects the priorities of the National Data Guardian (NDG) and is particularly concerned with the management of patient information, ensuring that it is safeguarded securely and used properly.

The Guardian shall:

- ensure that the Trust satisfies the highest practical standards for handling patient identifiable information;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion IG requirements and issues at board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for Employees;
- ensure that information sharing protocols and agreements are established with partner organisations where confidential patient information may be shared across organisational boundaries;
- provide a focal point for patient confidentiality and information sharing issues.

Data Protection Officer

The Data Protection Officer (DPO) is responsible for ensuring that the Trust and its constituent business areas remain compliant at all times with Data Protection, Privacy &

Electronic Communications Regulations, Environmental Information Regulations, and associated legislation.

The DPO shall be the Trust's first point of contact for the Information Commissioner's Office (ICO).

The DPO also has the responsibility:

- to ensure the IG Development Plan and delivery is in line with legal and national requirements;
- to inform and advise the organisation (Executive and Trust Board) and its Employees about their obligations to comply with the GDPR and other data protection laws;
- via the IGSG - to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training Employees and conducting internal audits; and
- to oversee the process underlying Subject Access Requests (SARs) as set out in the SOP4 - Subject Access Request.

Information Governance Steering Group
The IGSG is accountable to the Integrated Digital Committee, and holds overall responsibility to ensure the Trust adheres to the Information Governance Policy.

The IGSG agenda is structured to monitor compliance with the National Data Security Standards (above) and sign-off completion of the NHS Digital DSPT.

The IGSG will receive regular reports of incidents, analysis of trends, and review copies of Incident Management Reports to ensure the mitigation of the risk and share learning across the Trust.

The Terms of Reference for the IGSG can be found in Appendix 3, which includes the full membership, reporting structure and administrative arrangements.

Line Managers
All Line Managers are responsible for:

- implementing good IG and information security practice into normal day-to-day activity;
- adhering to IG and DSP related procedures;
- ensuring, with their IAO, that breaches and near misses relating to Trust information, data and/or systems are reported in accordance with the Information Security Policy; and
- ensuring that they, their Employees and teams attend the required training regarding information security, handling and Governance.

All Employees
Everyone has a duty to respect a data subject's right to confidentiality. All Employees and anyone working on behalf of the Trust involved in the receipt, handling or sharing of information held by the Trust, including personal identifiable information, shall adhere to this Policy to support the reputation of the Trust and, where relevant, of their profession.

All Employees starting work with the Trust are informed that by accessing Trust systems they are agreeing to adhere to the requirements of Trust policies, which will apply indefinitely during and after their employment with the Trust.

All Employees shall report information security incidents, as set out in the Information Security Policy.

All Employees shall undertake the required Data Security Awareness training for their role.

All Employees shall rescind access to information and any related equipment on completion of their role.

Third Parties
Risks to the Trust's information and information processing facilities shall be identified and managed prior to granting third-party access.

All contracts shall contain an appropriate Information Governance and Confidentiality clause. This shall include a requirement to provide assurance to the Trust regarding the secure handling of information held or processed on its behalf. Details are set out in the Information Security Policy under, Third Party and Suppliers.

6. Policy

This Policy sets out the approach taken within the Trust to provide a robust Information Governance (IG) Management Framework, for the current and future management of information, and compliance with required legislation.

Information Governance comprises a set of requirements relating to how organisations should process information, and the accountabilities concerned. The requirements cover all information held and processed by, or on behalf of, the Trust including, but not limited to Employee and patient personal information, as well as corporate information such as financial, contractual, and accounting records.

Any associated resource implications incurred by the implementation of the IG Policy, will be identified by the IG Steering Group, and reported to the Trust's Board as appropriate and required.

This Policy sets out to further develop and implement a change in culture towards IG by all Employees. IG is a key component of performance management, i.e. it is central to the working practices of all Employees, of all grades and roles, permanent or temporary, working within the Trust.

Legal and Regulatory Framework

There are a number of legal obligations placed upon the Trust for the use and security of personal and confidential information.

The main Acts of UK Parliament, and guidance documents relating to Information Governance, are:

- The Common Law Duty of Confidentiality;
- Confidentiality: NHS Code of Practice;
- NHS Care Record Guarantee for England;
- Social Care Record Guarantee for England;
- The international information security standards: ISO/IEC 27002: 2013, ISO/IEC 27001: 2013; BS 7799;
- Information Security Management: NHS Code of Practice;
- Records Management: NHS Code of Practice;
- The Freedom of Information Act 2000;
- The Computer Misuse Act 1990 (and subsequent amendments);
- The Human Rights Act 1998;
- The Caldicott Report 1997 - Report on the review of patient-identifiable information;
- Information: To Share or Not to Share? The Information Governance Review 2013 (also known as Caldicott 2 Recommendations);
- NHS Information Governance – Guide on Legal and Professional Obligations;
- Information Security Management: NHS Code of Practice;
- The Data Protection Act (1998) and subsequent Act (2018). This enshrines in UK law the provisions of the EU General Data Protection Regulation (GDPR);
- The Network and Information Systems Regulations, transposed into UK law in 2018;
- The Government Functional Standard for Security (Minimum Cyber Security Standard) 2018;
- The National Cyber Security Policy 2016;
- The NHS Data Security and Protection Toolkit (DSPT).

The Trust is registered with the Information Commissioner's Office as a Data Controller and processor of information and must comply with its duties as defined by this registration.

There is a mandatory requirement that all Trusts and providers to the NHS complete an annual return under the NHS Data and Security Protection Toolkit (DSPT). This aims to ensure that the ‘10 Data Security Standards’ set out by the National Data Guardian are being met. NHS Trusts are expected to provide a Declaration of Maturity regarding information handling, to be included in their Annual Report.

Information security also forms part of the Care Quality Commission (CQC) inspection regime under key line of enquiry W6[1]. The annual publication of assessments regarding data and Information security and protection is a contractual requirement under NHS England’s standard conditions contract.

Further obligations under the Data Protection Act 2018 are set out in the Confidentiality & Data Protection Policy.

Compliance

This Policy shall be reviewed against the Data Security and Protection Toolkit (DSPT) to identify key areas for continuous improvement. Amendments may also be made in response to significant changes due to security incidents, variations of law and/or changes to organisational or technical infrastructure.

Compliance with this Policy shall be monitored by internal and external audits commissioned by the Executive Team and reflect the Information Risk Appetite of the Trust.

Failure to comply with this Policy may result in breaching the GDPR/Data Protection Act (and other legal and regulatory) requirements, resulting in a fine from the Information Commissioner. Where there is a breach of confidentiality or loss of data or Information Asset, this must be reported and managed as per the Information Security Policy.

The Information Governance Group (IGSG) is responsible for ensuring an assessment of compliance, as detailed in the DSPT is undertaken each year. Annual work / development plans are produced, and these are considered by the IGSG at intervals throughout the year and reviewed before submission as per the deadlines below:

- Baseline – 31st October
- Submission of self-assessment for the year – 30th June

Reports on progress are provided to the SIRO, DPO and Caldicott Guardian, via the IGSG and the Integrated Digital Committee as required.

[1] 1. CQC Key Lines of Enquiry - https://www.cqc.org.uk/guidance-providers/healthcare/management-information-healthcare-services

7. Training

The National Data Guardian (NDG) Review requires that all NHS Employees undertake appropriate annual Data Security Awareness training and pass a mandatory test. This includes non-permanent Employees that have access to personal confidential information. To meet this mandatory requirement, ongoing awareness and training shall be provided to all Employees, in all Departments and Units of the Trust:

- Data Security Awareness Training shall be included throughout the Employee lifecycle;
- Annual update training shall be provided for all clinical and non-clinical Employees;
- the Trust shall routinely promote awareness relating to IG at Senior Team Briefs and electronically to all Employees via internal communication methods. This should include online courses and WebEx seminars available through NHS Digital.[2]

Permanent new Employees will receive Data Security Awareness training as part of their Induction via an on-line e-Learning package with eAssessment. Face-to-face bespoke training is also available on request from the Education & Training Team to meet learning needs.

Annual mandatory online e-Learning Data Security Awareness training is required for all employed Employees (both permanent and temporary). This is available from the e-LfH training tool and links directly to an individual's training record. Facilitated face-to-face sessions are available on request from the Education & Training Team for Employees who do not have access to a computer or require additional training support.

In addition, some roles are required to complete additional annual training, (e.g. the DPO, SIRO, Caldicott Guardian and IT Security Specialist) which is available via the NHS Digital e-Learning site.

Compliance with the mandatory annual training is included in all services' Performance Review Dashboards and monitored at Division Performance Reviews and at the IGSG.

See appendix 3 – Training TNA.

8. Stakeholder Engagement and Communication

This policy has been developed in accordance with the Cyber Operational Readiness Support teams, and the members of the Information Governance Steering Group.

[2] Online learning resources are available at: https://nhsdigital.e-lfh.org.uk/

9. Approval and Ratification

The policy will be approved and ratified by the Information Governance Steering Group.

10. Dissemination and Implementation

The policy will be disseminated through the Aspire global email and published on the organisation intranet and internet sites.

The Information Governance Steering Group is responsible for the implementation of this policy, including monitoring compliance.

11. Review and Revision Arrangements

This policy will be reviewed every year in line with Trust policy; or updated in line with any new legislation issued or change in procedures; or when there is a change in national IG policy or guidance.

12. Document Control and Archiving

This Policy is written by the IG Manager and maintained by the SIRO on behalf of the Board. Questions relating to its content or application should be addressed through the Information Governance Structure to the SIRO who is responsible for facilitating communication of this Policy throughout the organisation. This Policy will be subject to review on an annual basis (or sooner if new legislation or codes of practice of national standards are introduced).

This is a Trust-wide document and archiving arrangements are managed by the Quality Department, which can be contacted to request master/archived copies.

13. Monitoring compliance with this Policy

Measurable Policy Objective	Monitoring/ Audit method	Frequency of monitoring	Responsibility for performing the monitoring	Monitoring reported to which groups/ committees, inc responsibility for reviewing action plans
As a Foundation Trust, and as stipulated in the Operating Framework, the Trust is required	The Data Security & Protection Toolkit annual self assessment is	Progress is monitored via the DSPTK Action Plan with status updates	IG Manager	Information Governance Steering Group

to be compliant with the DSPT. Failure to maintain this would mean that the Trust would be unable to tender for new business.	monitored by the IGSG.	provided against each mandatory standard and reviewed on a bi-monthly basis.		

14. Supporting References / Evidence Base

Effective information security is delivered through a combination of people, policies, processes and technology. This Information Governance Policy is supported by a range of policies, from board level through to operational guidance, which provide more detail on the way in which these different aspects are managed. These Policies are available on the Trust's intranet and/or via Line Managers. They include, but are not limited to:

- Acceptable Use Policy;
- Confidentiality & Data Protection Policy;
- Information Governance Policy;
- Information Security Policy.
- Business Continuity Plan;
- SOP 3 - Subject Access Requests;
- SOP 4 – Incident Management;
- Cyber Incident Response Procedure
- Incident Reporting Policy

Useful links:

Data Security & Protection Toolkit: https://www.dsptoolkit.nhs.uk/

Information Commissioners Office: https://ico.org.uk/
Data Protection Act 2018

Freedom of Information Act 2000

National Archives (Public Records):http://www.nationalarchives.gov.uk/information-management/

Records Management Code of Practice

Caldicott2 Review: Caldicott review: information governance in the health and care system - GOV.UK (www.gov.uk)

National Data Guardian: National Data Guardian - GOV.UK (www.gov.uk)

Care Quality Commission: http://www.cqc.org.uk/

CQC Key Lines of Enquiry - https://www.cqc.org.uk/guidance-providers/healthcare/management-information-healthcare-services

Online learning resources are available at: https://nhsdigital.e-lfh.org.uk/

Appendix 1: Information Governance Steering Group

Terms of Reference

1. Introduction

Information Governance provides a framework to bring together the requirements, standards and best practices that apply to the handling of information; ensuring information is accurate, dealt with legally, securely and efficiently in order to deliver the best possible care.

The Principles of Information Governance (IG) include:

- Compliance with Data Protection law (including the General Data Protection Regulation – GDPR);
- Information Governance Policies and Procedures, including compliance with the 10 National Data Security Standards;
- Data Security and Cyber Management;
- Confidentiality and Caldicott Guidance;
- Data Quality;
- Secondary Use; and
- Corporate Information Management.

2. Purpose

The purpose of the Information Governance Group (IGSG) is to:

- provide a forum for the discussion, acknowledgement and sign off of the IG Management Framework;
- review and sign off policies and procedures as required by the IG Management Framework;
- review Caldicott/confidentiality issues, including access to electronic systems; review of incidents relating to breaches of confidentiality and other issues as required;
- ensure compliance with NHS Digital Data Security & Protection Toolkit (DSPT) assurances, including mandatory training compliance; and
- share knowledge and learning from IG incidents, and issues raised by the Information Commissioner's Office.

The group will provide advice and assurance to the Trust on all matters concerning Information Governance and will coordinate, supervise and direct the work necessary to provide a co-ordinated corporate approach to Information Governance.

Accountable to the Trust Board via the Data Protection Officer (DPO), SIRO and Caldicott Guardian, bi-monthly updates will be made to the Integrated Digital Committee to coincide with the national DSPT submissions; and IG contribution to Trust Board**.**

The Group will receive reports on Caldicott/confidentiality issues, Data Quality, Records Management, Freedom of Information, Directorate/Service/ISD IG Groups, Incidents, Asset Register Management, IG Risk Management, Information Security and cyber developments, Information Sharing Protocols and Data Protection Impact Assessments.

3. Objectives

The objectives of IGSG include:

the provision of a Trust-wide effective suite of Information Governance Policies, procedures, guidance and management arrangements which are regularly reviewed in line with changes in legislation and regulatory requirements, including:

- maintaining a balance between openness and confidentiality;
- legal compliance (e.g. Data Protection, Freedom of Information and other relevant legislation);
- Information Security (including Cyber Security, confidentiality, information sharing, integrity and availability);
- information quality assurance; and
- records management.

ensuring compliance with the DSPT ensuring all 10 Data Security Standards are met and evidence is uploaded into the NHS Digital online tool;

compliance with Care Quality Commission Standards, NHSLA Standards, Department of Health Codes of Practice, Clinical Negligence Scheme for Trusts, the ISN for Information Governance;

ensuring compliance with the recommendations and commitments identified in the Caldicott 2 Review;

providing support and structure to the DPO, Senior Information Risk Owner (SIRO), the Caldicott Guardian, and the Head of Information Assurance and Information Assurance Team;

developing and maintaining an IG Development Plan to address all Information Governance improvements, including securing necessary resources and monitoring the implementation of the plan;

providing reports to the Information Management and Strategy Forum via the Delegated SIRO (Chair) regarding compliance with the DSPT annual submission (usually end of March);

receiving and approving Data Privacy Impact Assessments and Information/Data Sharing Agreements;

receiving and considering reports into breaches of IG/confidentiality and where appropriate undertake or recommend remedial action, including sharing learning and reporting on concerns raised by the Information Commissioner’s Office;

via the Information Asset Register, ensuring IG risks are identified, assessed, mitigated and regularly reviewed and when appropriate recorded on the Trust Risk Registers;

receiving requests and maintaining a register of Access Requests and Approvals to Electronic Patient Records Systems (e.g. PAS);

promoting Information Governance throughout the Trust Clinical and Corporate divisions via IG Leads, ensuring that all staff receive annual Data Security Awareness training.

4. Membership

Membership of IGSG will include:

a) Data Protection Officer (joint Chair);
b) Senior Information Risk Officer (SIRO (Chair);
c) Head of Information & Technology (joint Chair);
d) Caldicott Guardian;
e) Head of Digital Programme Delivery
f) Information Governance Manager;
g) Information Security Specialist;
h) Head of Information;
i) Head of Information Assurance;
j) Quality & Governance Manager;
k) FOI Lead);
l) Head of Estates and Facilities Management;
m) Head of Finance;
n) Senior HR Manager – Workforce Information & Systems;
o) Chief Clinical Information Officer (CCIO);
p) Divisional/Service Information Governance Leads (MH, LD, HR, Finance, Integrated Service Divisions, Children’s Services. See body of policy for role of IG Manager);
q) Learning, Education and Development Representative;
r) and others by invitation;
s) Deputies to attend as necessary to ensure all divisions are represented.

5. **Quorum**

This is constituted when the DPO, Caldicott Guardian (or Delegated Caldicott Guardian), SIRO (or Delegated SIRO) and Head of Information Assurance are present and at least 4 members as well.

6. Frequency of Meetings

Meetings will be bi-monthly or as required. The use of teleconferencing for sign off to be used as required.

Training Programme	Frequency	Course Length	Delivery Method	Facilitators	Recording Attendance	Strategic & Operational Responsibility

Data Security Awareness – Induction and Annual Re-fresher	Annually	Approx. 1 hour	eLearning or eAssessment via LEAD training tool	Information Assurance Team	Individual log-into system	Director of Information & Technology Head of Information Assurance

Directorate	Service	Target Audience
AMH/LD/OPMH	Adult Mental Health	All staff
	Specialised Services	
	Learning Disabilities	
	Older Persons Mental Health	
ISD's	Adults	
ISD's	Children's Services	
Corporate	All	

Appendix 2: Training Needs Analysis

APPENDIX 3: EQUALITY IMPACT ASSESSMENT

Equality Impact Assessment Summary

Name and title: Jane Townsend – Information Governance Manager
Policy: Information Governance Policy

Background • Who was involved in the Equality Impact Assessment
The Trust's IG Team and members of the Information Governance Steering Group.
Methodology • A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how?)
The policy was assessed as not impacting upon an individual's race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age. The information was a review of policy itself. Consultation was therefore considered not applicable in this case.
Key Findings • Describe the results of the assessment • Identify if there is adverse or a potentially adverse impacts for any equalities groups
No adverse or potentially adverse impacts have been identified for any equalities groups; the policy affects all staff equally.
Conclusion • Provide a summary of the overall conclusions
As outlined in methodology section.
Recommendations • State recommended changes to the proposed policy as a result of the impact assessment

- Where it has not been possible to amend the policy, provide the detail of any actions that have been identified - Describe the plans for reviewing the assessment
No changes recommended.

APPENDIX 4: CHECKLIST FOR THE REVIEW AND APPROVAL OF DOCUMENTS

To be completed (electronically) and attached to any document which guides practice when submitted to the appropriate committee for approval or ratification.

Title of the document: Integrated Identity Management (RA) Policy
Policy (document) Author: Nicki Rayment – Head of Digital Programme Delivery
Executive Director: Simon Marshall – Director of Finance

		Yes/No/ Unsure/ NA	**Comments**
1.	**Title**		
	Is the title clear and unambiguous?		
	Is it clear whether the document is a guideline, policy, protocol or standard?		
2.	**Scope/Purpose**		
	Is the target population clear and unambiguous?		
	Is the purpose of the document clear?		
	Are the intended outcomes described?		
	Are the statements clear and unambiguous?		
3.	**Development Process**		
	Is there evidence of engagement with stakeholders and users?		
	Who was engaged in a review of the document (list committees/ individuals)?		
	Has the policy template been followed (i.e. is the format correct)?		
4.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?		
	Are local/organisational supporting documents referenced?		
5.	**Approval**		
	Does the document identify which committee/group will approve/ratify it?		
	If appropriate, have the joint human resources/staff side committee (or equivalent) approved the document?		
6.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?		
	Does the plan include the necessary training/support to ensure compliance?		

		Yes/No/ Unsure/ NA	Comments
7.	**Process for Monitoring Compliance**		
	Are there measurable standards or KPIs to support monitoring compliance of the document?		
8.	**Review Date**		
	Is the review date identified and is this acceptable?		
9.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?		
10.	**Equality Impact Assessment (EIA)**		
	Has a suitable EIA been completed?		

Committee Approval (insert name of Committee)			
If the committee is happy to approve this document, please complete the section below, date it and return it to the Policy (document) Owner			
Name of Chair	**Laura Ellis-Philip**	**Date**	
Ratification by Management Executive (if appropriate)			
If the Management Executive is happy to ratify this document, please complete the date of ratification below and advise the Policy (document) Owner			
Date: n/a			