Information Governance Policy (N-008)

Version Number:	3.12
Author (name & job title)	Lisa Davies, Head of Information Governance and Legal Services and Data Protection Officer
Executive Lead (name & job title):	Peter Beckwith, Senior Information Risk Owner
Name of approving committee:	Quality Committee
Date approved:	7 February 2018
Date Ratified at Trust Board:	28 February 2018
Next Review date:	December 2024

Policies should be accessed via the Trust internet to ensure the current version is used.

Minor amendments made prior to review date (see appended document control sheet for details)	
Date:	*17 November 2021*
Approved by:	*Information Governance Group*
Date Approving Committee notified for information:	*February 2022 (Audit Committee)*

Contents

1. INTRODUCTION

Information is a vital asset, both in terms of the clinical management of individual service users and the efficient management of services and resources of the Trust. It plays a key part in clinical governance, service planning and performance management.

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

The way in which the Trust will deliver against these requirements is described in this policy and forms the Trust's Information Governance Management Framework. As required by the Data Security and Protection Toolkit the adequacy of the IG Management Framework must be reviewed on an annual basis to ensure it remains fit for purpose.

2. SCOPE

This policy applies to all employees of the Trust, all Social Services mental health staff who are seconded to the Trust, contract and agency staff and other people working and volunteering at the Trust.

3. DUTIES AND RESPONSIBILITIES

Chief Executive
The chief executive as accountable officer has overall accountability and assurance, through the Statement of Internal Control that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner
The Senior Information Risk Owner (SIRO) will be the senior manager with Board level responsibility for information governance.

The SIRO will act as an advocate for information risk and provide written advice to the Accountable Officer on the content of their annual Statement of Internal Control in regard to information risk.

Head of Information Governance and Legal Services and Data Protection Officer
The head of information governance and legal services will:

- Be the overall information governance lead and co-ordinate the IG work programme;
- Develop and maintain appropriate documentation that demonstrates commitment to and ownership of IG responsibilities;
- Ensure there is top level awareness and support for IG resourcing and implementation of improvements;
- Provide direction in formulating, establishing and promoting IG policies;
- Co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- Ensure annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
- Ensure that annual assessment and improvement plans are prepared for approval by the Information Governance Committee in a timely manner;
- Ensure that the approach to information handling is communicated to all staff and made available to the public;
- Ensure that appropriate training is made available to staff and completed as necessary to support their duties and in line with the requirements of the Informatics Planning component of the NHS Operating Framework 2010/11;
- Liaise with other committees, working groups and programme boards in order to promote and integrate IG standards;

- Monitor information handling activities to ensure compliance with law and guidance;
- Provide a focal point for the resolution and/or discussion of IG issues.

Caldicott Guardian
The Caldicott Guardian will:

- Be the senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing;
- Play a key role in ensuring that the Trust satisfies the highest practicable standards for handling patient identifiable information.

Clinical Leads
Clinical leads will be responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

Trust Staff
All Trust staff (whether permanent or temporary) and contractors/volunteers are responsible for ensuring that they are aware of the requirements incumbent upon them in the Information Governance policy and supporting standards and guidelines, and for ensuring that they comply with these on a day to day basis.

Corporate data quality objectives will be included in updated job descriptions for all staff. Delivery of these responsibilities will be assessed as part of the annual staff performance and development review.

Key Governance Bodies

Audit Committee
The Audit Committee will:

- Endorse and approve the Trust's information governance management framework, taking into account legal and NHS requirements;
- Sign off the Annual Report and information governance improvement plan and work programmes.

Information Governance Group
The Information Governance Group will:

- Comprise senior representatives from across the Trust and its professional disciplines to promote a holistic approach to IG;
- Be responsible for the overall IG agenda and ensure that the Trust has effective policies and management arrangements covering all aspects of IG;
- Establish an annual Information Governance Improvement Plan, securing the necessary implementation resources and monitoring the implementation of that plan;
- Receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action.

4. PROCESS

Policies
This policy is supported by other more detailed policies covering specific aspects of the information governance agenda.

They are:

- Caldicott and Data Protection Policy
- Information Security Policy
- Access to Health Records Policy

- Confidentiality Code of Conduct
- Electronic Communications and Internet Acceptable Use Policy
- Freedom of Information Act Policy
- Safe Haven Procedure
- Health and Social Care Records Policy
- Records Management and Information Lifecycle Policy
- Information Governance and IT Forensic Policy

Resources
Key staff roles with dedicated budget are responsible for the following functions:

Data Protection and Training
Information governance officer/information governance support officer.

Information Security
The head of information governance and legal services is responsible for policy and ensuring there is an overall framework for information security. Digital information security will be delivered by the head of digital delivery and health chief information officer.

Information Asset Register, Toolkit Compliance, IG Compliance at Unit Level, Privacy Officer Role
Information governance lead.

Freedom of Information
The head of information governance and legal services supported by the information governance and legal team.

Data Quality
The deputy director of business and contracting is responsible for policy and ensuring there is an overall framework for data quality assurance, delivered by the information management lead.

Registration Authority
Head of digital delivery and health chief information officer.

Governance Framework
IG responsibility and accountability will be cascaded through the Trust by the following means:
- Outlined in staff contracts
- Specified in contracts with third parties
- Staff sign up to the Confidentiality Code of Conduct
- Identification of Information Asset Owners at departmental level

Training and Guidance
Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures.

The approach to the Trust ensuring that all staff receive training appropriate to their roles is detailed in the Information Governance Training Procedure.

Incident Management
The investigation of incidents will follow the guidance issued by the NHS Digital's Guide to the notification of data security and protection incident.

The way in which information governance relates to the Trust's integrated governance framework, in respect of risk, is described in the Trust's Risk Management Strategy.

The Assistant Director of Nursing, Patient Safety and Compliance is responsible for information related to all risk management. The a Assistant Director of Nursing, Patient Safety and Compliance will inform the Trust's SIRO and Caldicott Guardian of any reportable incidents and ensure that information related incidents are investigated and that lessons are learned and communicated across the Trust. The Assistant Director of Nursing, Patient Safety and Compliance directly to the director of nursing.

The Assistant Director of Nursing, Patient Safety and Compliance, supported by the Head of Information Governance and Legal Services is also responsible for analysing trends to inform care groups' decisions, particularly:

- Escalating serious incidents to the SIRO.
- Analysing trends to inform information management decisions.
- Supporting reviews of serious incidents regarding information.
- Advising on the need for independent investigations by external agencies or individuals relating to information.

Reporting
The head of information governance and legal services will ensure that there are adequate arrangements in place for:

- Reporting IG events or incidents, e.g. information quality failures, actual and potential breaches of confidentiality or information security.
- Analysing, investigating and upward reporting of events/incidents and any recommendations for remedial action.
- IG work programme progress reports.
- Reporting annual IG assessment and improvement plans.

Communicating IG developments and standards to the IG Group.

5. CONSULTATION

Consultation regarding this policy has taken with Information Governance Group.

6. IMPLEMENTATION AND MONITORING

This policy will be disseminated by the method described in the Document Control Policy. This policy does not require additional financial resource.

The provision of reasonable adjustments that may be implemented as a result of this policy will be supported by the Trust.

This policy will be monitored and audited via the annual Data Security and Protection Toolkit assessment.

7. TRAINING AND SUPPORT

Information governance training will be provided to all staff as detailed in the Information Governance Training Procedure.

8. REFERENCE TO ANY SUPPORTING DOCUMENTATION

Data Security and Protection Toolkit: Evidence item 1.2.1: There is a data security and protection policy or policies that follow relevant guidance.

NHS Digital's Guide to the notification of data security and protection incident.

Appendix 1: Document Control Sheet

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Policy – Information Governance Policy		
Document Purpose	This policy and associated Standard Operating Procedure provides a framework that has transformed culture, leadership and professional practice to deliver care and support which keeps people safe, and promotes recovery.		
Consultation/ Peer Review:	Date:	Group / Individual	
List in right hand columns consultation groups and dates	November 2021	Information Governance Group	
Approving Committee:	Quality Committee	Date of Approval:	7 February 2018
Ratified at:	Trust Board	Date of Ratification:	28 February 2018
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*		Financial Resource Impact	
Equality Impact Assessment undertaken?	Yes [✓]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [✓]
Master version held by:	Author [ ]	HealthAssure [✓]	
Implementation:	*Describe implementation plans below - to be delivered by the author:*		
	• Dissemination to staff via global email • Teams responsible for ensuring policy read and understood		
Monitoring and Compliance:			

Document Change History:			
Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
3.04	Review	Aug 11	IG approval
3.05	Review	June 12	Job title changed to Information Governance and Legal Services Manager "Annual Assessment" changed to "Annual Report" Addition of role of Privacy Officer
3.06	Review	May 13	Job titles Introduction – addition of Toolkit standard 101 to review IG Framework on an annual basis. Data Quality responsibility Head of Innovation and Programmes RA responsibility Head of Organisational and Management Development
3.07	Review	April 14	Job titles amended 5. PROCEDURES, the incident reporting arrangements have been amended to reflect Health & Social Care Information Centre, revised Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation (01 June 2013)

3.08	Review	Sept 15	Job Titles and reporting arrangements amended. Removal of the role of CIO
3.09	Review	Sept 16	Under Bribery Act section, references and contact details updated
3.10	Review	Dec 17	Policy updated to revised Trust format, job titles updated and role of deputy director of governance and patient experience removed
		Sept-18	Approval committee change from Quality Committee to Audit Committee
3.11	Review	Dec 18	Updated reference to the revised NHS Digital Incident Reporting guidance and reviewed Data Security and Protection Toolkit.
3.12	Review	Nov 21	Updated job titles and inclusion of volunteers. Removal of the role of Freedom of Information Officer.

Appendix 2: Equality Impact Assessment

Equality Impact Assessment (EIA) Toolkit

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. Document or Process or Service Name: Information Governance Policy
2. EIA Reviewer (name, job title, base and contact details) Lisa Davies, Head of Information Governance and Legal Services, , Mary Seacole Building, 01482 477840
3. Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other? Policy

Main Aims of the Document, Process or Service
The Information Governance Policy describes the Trust's information governance management and accountability structures, governance processes, documented policies and procedures, staff training and resources.
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender reassignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	**Low**	The policy is the overarching document which describes how the Trust will meet its Information Governance requirements. Specific areas of information governance are covered in standalone policies (for example the Caldicott and Data Protection Policy) and these policies have been separately impact assessed. The IG issues log and quarterly reports to the IG Committee are scrutinised and any issues arising which relate specifically to equality impact would be identified through that process.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical	**Low**	As above

	Learning Mental health (including cancer, HIV, multiple sclerosis)		
Sex	 Men/Male Women/Female	**Low**	As above
Marriage/Civil Partnership		**Low**	As above
Pregnancy/ Maternity		**Low**	As above
Race	Colour Nationality Ethnic/national origins	**Low**	As above
Religion or Belief	All religions Including lack of religion or belief and where belief includes any religious or philosophical belief	**Low**	As above
Sexual Orientation	Lesbian Gay men Bisexual	**Low**	As above
Gender reassignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	**Low**	As above

Summary

Please describe the main points/actions arising from your assessment that supports your decision above There is no evidence of potentially negative effect on groups in the categories above. No issues have been identified from patient focus groups, PALS & Complaints, CQC inspections, staff surveys.	
EIA Reviewer: Karen Robinson	
Date completed: 20 February 2019	Signature: K Robinson