Gloucestershire Hospitals
NHS Foundation Trust

TRUST POLICY

INFORMATION GOVERNANCE

This document may be made available to the public and persons outside of the Trust as part of the Trust's compliance with the Freedom of Information Act 2000.

Please be aware that only documents downloaded or viewed directly from the GHNHST Trust Policies webpage are valid documents. Documents obtained through printed copies or internet searches may be out of date and therefore will be invalid.

In this document you may find links to external websites. Although we make every effort to ensure these links are accurate, up to date and relevant, Gloucester Hospitals NHS Trust cannot take responsibility for pages maintained by external providers.

FOR USE BY:

This document is to be followed by all staff of Gloucestershire Hospitals NHS Trust

FAST FIND:

- AC1 – Removal of Consent to use Personal Information for Non-Clinical Purposes

- B0413 AC1 Removal of Consent to use Personal Information for Non-Clinical Purposes
- Gloucestershire Information Sharing Partnership Agreement (GISPA)
- Data Security and Protection Toolkit
- Clinical and Non-Clinical Information Systems Management Policy (B0676)
- Data Quality Policy

1. INTRODUCTION / RATIONALE

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

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

2. DEFINITIONS

Word/Term	Descriptor
Information Governance	Information Governance is the framework of law and best practice that regulates how information (including information relating to and identifying individuals) is managed, i.e. obtained, handled, used and disclosed.
Information Governance Assurance Framework	The Information Governance Assurance Framework (the "Framework") is a national framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the NHSE Data Security and Protection Toolkit (DSPT) and cover the following areas: • Access to information (Freedom of Information Act 2000 and Subject Access Requests) • Confidentiality and Data Protection • Information security assurance • Information quality assurance - Records Management It also includes the NHS Framework for Shared Care Records
Data Protection Legislation	The UK General Data Protection Regulation, the Data Protection Act 2018, and the common law duty of confidentiality
NHSE	NHS England. Lead organisation for the management of the NHS in England. From 01 February 2023 NHS Digital (NHSD) merged with NHSE. All references in IG resources to NHSD or to HSCIC (Health and Social Care Information Centre) should now be read as references to NHSE

3. POLICY STATEMENT

This policy applies to all staff whether permanent, temporary, volunteers, or contracted staff, including contractors that are employed directly or otherwise by the Trust.

The aim of this policy is to define the framework and set the standards expected throughout the Trust for the use and management of information and to brief staff on the trust's IG requirements, outline the training provision, reporting structure, risk and incident management processes and the annual IG work plan and give assurance to the Trust and to individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

This policy covers all aspects of information management within the Trust, including:

- Patient/Client/Service User information
- Personnel information
- Organisational information

And all aspects of handling information, including:

- Structured and unstructured record systems - paper and electronic
- Transmission of information – e.g. e-mail, post, telephone, removable media
- Sharing of Information to third parties

Information Governance provides a way for the Trust to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Legislation.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2022 and ISO/IEC 27001:2022.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice 2021.
- The Freedom of Information Act 2000.
- The Human Rights Act article 8.
- The 'Report on the review of patient-identifiable information' (alternative title 'The Caldicott Report') and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review).
- Information: To share or not to share - Government Response to the Caldicott 2 Review.
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-Outs (also known as Caldicott 3 Review)
- The EU Directive on the security of Networks and Information Systems (NIS Directive)
- Information Governance Framework for Integrated Health and Care

4. ROLES AND RESPONSIBILITIES (Including Senior Roles and Governance Framework responsibility, accountability and resources)

Post/Group	Details
Trust Board	• To approve the Trust's Policy in respect of Information Governance, taking into account legal and NHS requirements. This role may be delegated to an appropriate sub-committee or executive director. • To receive a report at least annually on the Trust's Information Governance performance.
Trust Senior Information Risk Owner (SIRO) (Digital and Chief Information Officer)	• Named Executive Director on the Board with responsibility for Information Governance. • To undertake the role of Senior Information Risk Owner (SIRO) for the Trust • Chair of the Trust Information Governance and Health Records Committee • To appoint the Lead for Information Governance • To appoint a trust lead for Data Protection and Freedom of Information
Caldicott Guardian (Medical Director)	• Named Executive Director with responsibility for Caldicott and is a member and vice chair of the Information Governance and Health Records Committee.
Lead for Information Governance (Associate Chief Information Officer IG and Health Records) The lead is also the DPO.	• Overseeing day to day Information Governance issues • Developing and maintaining policies, standards, procedures and guidance • Co-ordinating Information Governance in the Trust and raising awareness of Information Governance • Co-ordination of the completion and annual submission of the DSPT • Lead on management of Information Governance Serious Incidents requiring • investigation (IG SIRI)
Data Protection Officer (DPO)	As required by Article 37 GDPR including: • to inform and advise the Trust and its employees of their obligations pursuant to the Data Protection Legislation • to monitor compliance with the Data Protection Legislation • to provide advice as regards data protection impact assessments and monitor their performance
Lead for FOI	• Overseeing day to day FOI issues • Developing and maintaining policies, standards, procedures and guidance • Co-ordinating and raising awareness of legal compliance
Information Governance Support and FOI Officer(s)	• Overseeing day to day FOI and DPA access to health record issues
Information Governance and	• Maintaining the currency of the Information Governance and Record Keeping policies and associated / complimentary policies and procedures.

Health Records Operational Group	
Digital care Delivery Group	• Accountable to the Trust Leadership Team via the Chair • Approving the results of information governance audits prior to presentation by the Trust Board
DSPT Standard Leads	• Assessing Information Governance performance against the DSPT Standards • Submitting results to NHSE on an annual basis via the DSPT as co-ordinated by the Lead for Information Governance • Responsible for cascading IG requirements within the organisation in relation to the IG Standard for which they are the lead
Managers	• To ensure that this Policy and any supporting documents are built into local processes • To ensure that the development of any new systems will be compliant with Information Governance requirements
All staff (see Policy Statement for Scope)	• To ensure that they are aware of Information Governance requirements and standards including data protection responsibilities in relation to their specific role and are compliant with these standards and responsibilities • To ensure that they complete IG and Code of Confidentiality mandatory training • To report IG related incidents including data breaches through the trust incident reporting tool Datix • To escalate any IG related concerns through their Line management and / or to the IG Lead
Information Asset Owners	• As set out in the Clinical and Non-Clinical Information Systems Management Policy (B0676)
System Managers (Information Asset Administraors	• As set out in the Clinical and Non-Clinical Information Systems Management Policy (B0676)

5. PRINCIPLES

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that 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 actively use information in decision making processes.

There are 4 key interlinked strands to the Information Governance Policy:

5.1 Openness

Non-confidential information on the Trust and its services should be available to the public through a variety of media.

- The Trust will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000
- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients
- The Trust will have clear procedures and arrangements for liaison with the press and broadcasting media
- The Trust will have clear procedures and arrangements for handling queries from patients and the public

5.2 Legal compliance

The Trust regards all identifiable personal information relating to patients and staff as confidential and as such takes steps to ensure that the handling of such information complies with the Data Protection Legislation .

- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements
- The Trust will establish and maintain policies to ensure compliance with the Data Protection Legislation and the Freedom of Information Act 2000.
- The Trust will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act 2012, Crime and Disorder Act 1998, The Children Act 2004)

5.3 Information security

The Trust will establish and maintain policies for the effective and secure management of its information assets and resources

- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements
- The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The Trust will maintain and review incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

5.4 Quality assurance

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

- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers and senior clinical staff are required to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality will be assured at the point of Collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

6. KEY POLICIES AND PROCEDURES

A full list of policies and procedures is available on the Trust intranet site Policy Library. Including Key Information Governance policies:

6.1 Information Governance Policy B0413

To brief staff on the trust's IG requirements, outline the training provision, reporting structure, risk and incident management processes and the annual IG work plan and give assurance to the Trust and individuals that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

6.2 IT Security Policy B0591

To ensure that electronic data is protected in all of its forms, during all phases of its life cycle, from unauthorised or inappropriate access, use, modification, disclosure or destruction, through the application of the standards and definitions of the ISO27000 series of standards as used in the DSPT.

The policy applies the key concepts of Information Assurance to electronic data processing in the Trust:

- Confidentiality
- Integrity
- Availability
- Accountability

6.3 Records Management Policy B0259

To ensure compliance with the legal and professional obligations set out in the Records Management: NHS Code of Practice 2021, in particular:

- The Public Records Act 1958;
- The Data Protection Legislation;
- The Freedom of Information Act 2000;

The NHS Confidentiality Code of Practice Including the management of access to health records requests and requests for information made under the freedom of Information Act 2000.

These and all other IG related policies are reviewed as required as part of the IG Strategy and annual improvement work plan.

6.4 The Data Protection and Security Toolkit (DSPT)

The annual information governance assessment is measured against the standards set out in the DSPT and is assured each year by Internal Audit. The Trust is required to submit three Information governance performance reports to the NHSE hich can be tracked by Commissioners and other monitoring bodies. The reporting deadlines are:

- Baseline assessment (28th February). The baseline does not have to meet a minimum standard and is an assessment of where the organisation is currently, in terms of self-assessment against the Standard.
- Final submission (30th June)

The final performance assessment submitted to NHSE is used by the Care Quality Commission as part of the Well Led inspection.

The results are also published on the DSPT website and made available to the general public.

6.5 The HSCN Connection Agreement

The Health and Social Care Network (HSCN) is the data network for health and care organisations. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently.

To access the HSCN the Trust has signed a connection agreement with NHSE under which it agrees to meet specified standards including:

- The right of audit by NHSE or nominated third parties
- Change Control Notification procedures and approval processes
- the implementation of robust data handling and information security practices reporting security events and incidents
- Allowing network monitoring by the HSCN authority

6.6 Data Protection Impact Assessments

Proposed changes to the Trust's processes and/or information assets involving personal data will be assessed. All changes will require a Data Protection Impact Assessment screening to be submitted to Information Governance. Changes assessed as being potentially high risk will undergo a full impact assessment with a view to reducing and mitigating risks. The aim is to ensure that the confidentiality, integrity and accessibility of personal information are maintained. Further information will be found in the Data Protection and Confidentiality Policy (B0734).

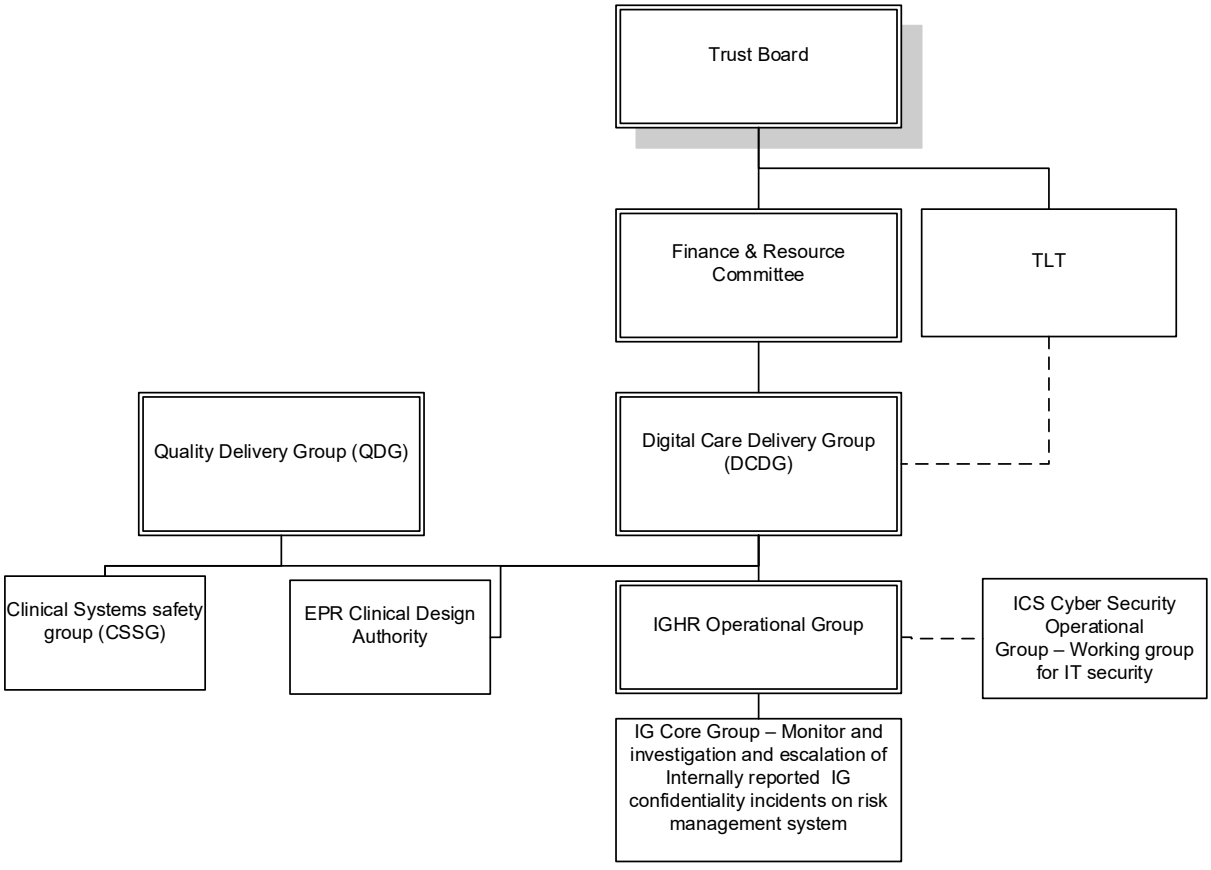
Where appropriate a change will also need to be submitted to CITS as a system change / new system.

6.7 Information Asset Register

The Trust will maintain an Information Asset register and records of data flows. Registers of data processing agreements and information sharing agreements may be maintained separately until incorporated into the main asset register.

7. KEY GOVERNANCE BODIES

Information Governance Reporting Structure



7.1 Digital Care Delivery Group (DCDG)

DCDG has responsibility for overseeing the implementation of this Information Governance Policy and Framework, the annual DSPT assessment and the annual Information Governance improvement plan. DCDG also reviews and approves all IG-related policies and procedures.

7.2 Information Governance and Health Records Operational Group

The IGHR OG maintains the currency of the Information Governance and Record Keeping policies and associated / complimentary policies and procedures.

7.3 IG Core Group

The group meets monthly for monitoring, investigation and escalation of internally reported IG confidentiality incidents on risk management system

7.4 Data Quality

Reporting and oversight is via the Quality Delivery Group which reports on matters of safety, effectiveness and patient experience via the Trust Leadership Team to a Quality and Performance Committee.

7.5 EPR Clinical Design Authority

Control panel for the development and control of electronic and legacy paper clinical documentation

7.6 Cyber Security Operational Group

Proactive management and development of IT security

8. TRAINING

Success in achieving compliance to the standards set out in the IG Framework is dependent on developing an Information Governance aware and knowledgeable work force.

Information Governance Training is incorporated into the Trust's Mandatory Training programme. It is a mandatory requirement for all GHNHSFT staff without exception to undertake annual Information Governance training which is appropriate to their role.

Different levels of training need to be completed by staff, as part of their mandatory training, depending on role and is viewable through the online training matrix.

All staff receive Information Governance awareness training as part of their corporate induction programme.

In subsequent years staff complete either a basic level training or a more advanced training depending on their job role. A Training Needs Analysis will be undertaken and kept under review to ensure that staff receive training appropriate to their Information Governance responsibilities.

9. INCIDENT MANAGEMENT

The Trust has an electronic reporting system for all incidents including IG related incidents and also offers a hotline number for anonymous reporting. IG confidentiality incidents are reviewed at the monthly IG core subgroup, where any required IG team support and intervention is made.

B0393 - Incidents - Managing, Reporting and Reviewing of Incidents / Accidents, including Serious Incidents

The Trust Incident Reporting System is designed to notify the Trust IG Lead and other members of the IG core subgroup of all occasions where information breaches are reported by trust staff members. This informs the scheduled meeting of the group of issues to be reviewed and also allows for more immediate action where this is required. This is in addition to the local management of incidents by the department or service lead where the incident has occurred.

IG incidents are assessed using the criteria set out in the HSCIC document: ”Guide to the Notification of Data Security and Protection Incidents (SIRI Guide)". If confirmed as an IG SIRI, they are graded for significance and likelihood using the guidance and reported to the ICO via the incident reporting section of the DSPT if the reporting threshold is met.

10. MONITORING OF COMPLIANCE

The SIRO, as sponsoring director, will agree with the DCDG a method for monitoring the dissemination and implementation of this policy.

Do the systems or processes in this document have to be monitored in line with national, regional or Trust requirements?	YES

Monitoring requirements and methodology	Frequency	Further actions
Data quality Audit Data Quality Team	Annually	Reported to DCDG

Data Protection Officer	Annually and as required	Trust Board
Legal Compliance Report Lead for Data Protection and FOI	Annually	Reported to DCDG Subject to ICO action dependent on severity of non-compliance
As an Acute Trust we are required to provide assurance using the DSPT that we are practising good data security and that personal information is handled correctly..	Annually	The Trust's information governance performance is measured through the baseline, improvement and annual DSPT reports and reported to the DCDG. It is included in the trusts Quality report and a final position paper is submitted to the Trust board prior to final submission each year.
Incidents reported on Datix monitored IG Core Group (Sub-committee)	Bi-monthly	IG SIRI escalated
IG SIRI monitored within Datix incidents as above, escalated to SIRO and reported in addition via the Data Security and Protection Incident Reporting tool of the DSPT	Annually and at time of incident	Reported to DCDG, Annual IG trust board report and section included in the Trust Quality Report. Qualifying incidents reported to ICO and NHS England through IGT. Subject to ICO action dependent on severity
IT Security Incidents Audit, IM&T Programme Manager	Annually	DCDG
Essential Standards of Quality and Safety The Care Quality Commission (CQC) will cross-check the Trust's DSPT submission as part of the assurance that the Trust is meeting the essential standards of quality and safety. This is measured against Quality and Risk Profiles and Key lines of enquiry including.	Annually	Reported through the Quality Standards Review Group

11. REFERENCES (The Trust is not responsible for the content of external websites)

NHS Information Governance: Guidance on Legal and Professional Obligations (2007) - NHSE

General Medical Council, Confidentiality, 2018

Health and Care Professions Council, 2020 Confidentiality – guidance for registrants

Health and Social Care Information Centre, 2013 A guide to confidentiality in health and social care and References Document Version 1.1 HSCIC

NHS Information Governance Framework for Shared Care Records NHSx September 2021

Health and Social Care Information Centre, July 2018 Guide to the Notification of Data Security and Data Protection Incidents v 1.2

, Data sharing Code of Practice Information Commissioner's Office (2021)

UK General Data Protection Regulation

NIS Directive EU 2016 / 1148 European Parliament & Council

Data Protection Act 2018

Human Rights Act 1998

Crime and Disorder Act 1998

Computer Misuse Act 1990.

Regulation of Investigatory Powers Act 2000

Electronic Communications Act 2000

Freedom of Information Act 2000

Access to Health Records Act 1990

The Health Service (Control of Patient Information) Regulations 2002

Copyright, Designs and Patents Act 1988 (as amended by the Copyright computer programs regulations 1992)

Children Act 2004

DOCUMENT PROFILE	
Reference Number	B0413
Title	Information Governance
Category	Non-Clinical
Version	V7
Issue Date	OCTOBER 2023
Review Date	OCTOBER 2026
Owning Division	Corporate
Owning Specialty	Information Governance
Associated Specialities	Trustwide
For Use By	GHNHST & GMS STAFF
Author	Thelma Turner, Associate Chief Information Officer IG and Health Records (DPO)
Quality Assurance Group	DCDG IGHR Operational Group
Other Approving Groups	Digital Senior Leads
Local Approval Details	IGHR Operational Group 01/03/2023 DCDG 01/08/2023
TPAG Ratification	October 2023
Consultees	IGHR Operational Group DCDG
Dissemination Details	Upload to Policy Site; cascade via IGHR Operational Group, IGT standards leads and divisions.
Keywords	Information Governance, Data Protection, Freedom of Information, DSP Toolkit.
Equality Impact Assessment (EIA)	EIA
Related Trust Documents	AC1 – Removal of Consent to use Personal Information for Non-Clinical Purposes
Other Relevant Documents	Incidents – Managing, Reporting and Reviewing of Incidents/Accidents, including Serious Incidents CCTV: Usage and Code of Practice Control of Contractors Disciplinary Policy Mandatory Training Risk Management Framework Risk Assessment Procedure Media, Celebrity and VIP Visitors Gloucestershire Information Sharing Partnership Agreement (GISPA) Clinical and Non-Clinical Systems Management Policy Intellectual Property

	Confidential Communications IT Security Policy Data Quality Policy Records Management Link to the NHSE – Registration Authority IT Forensic Readiness Policy Portable IT Equipment and Removable Media Maternity Health Records Policy Storing and Sharing Electronic and Paper Records Data Protection and Confidentiality Research Governance
External Compliance Standards and/or Legislation	NHS Data Security and Protection Toolkit UK General Data Protection Regulation (GDPR) See also section 3 of policy for fuller list