Gloucestershire Hospitals
NHS Foundation Trust

TRUST POLICY

IT SECURITY

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 Documents obtained through printed copies or internet searches may be out of date and therefore will be invalid.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 and Gloucestershire Managed Services

FAST FIND:

This policy is a one of a number of the organisations Data security and Data protection policies and should be read in conjunction with the information governance and related polices available on in the organisations policy library.

This document is the IT Security Policy for Gloucestershire Hospitals NHS Foundation Trust and defines the recommended IT Security Policy for other stakeholders in the Gloucestershire Countywide IT Shared Service as per relevant SLA. It should be adopted as a corporate, non-clinical policy by each trust which participates in the shared service. The IT Security Policy applies to all business functions and information contained in electronic format within the Trust, the physical environment and people who administer, support and use the IT Service.

1. INTRODUCTION

This document is the IT Security Policy for Gloucestershire Hospitals NHS Foundation Trust and defines the recommended IT Security Policy for other stakeholders in the Gloucestershire Countywide IT Shared Service. It should be adopted as a corporate, non-clinical policy by each Trust which participates in the shared service as referenced in the security management plan as part of the SLA. This policy applies to all business functions and information contained in electronic format within the Trust, the physical environment and people who administer, support and use the IT Service.

This policy is supported by a framework of other documents covering aspects of the organisations change management, physical security, remote working and acceptable use available on in the organisations policy library .

Read this document in conjunction with the participating organisation's Information Governance Policies

- Gloucestershire Hospitals NHS Foundation Trust; Information Governance Policy (B0413)
- Gloucestershire Health & Care NHS Foundation Trust: Information Governance Management System Policy (IGMS).
- NHS Gloucestershire ICB: NHS Gloucestershire ICB: Data Security & Protection Policy (88)

The legal framework for this policy includes:

- The UK General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act (1990)
- Copyright Designs & Patents Act (1988)
- Regulation of Investigatory Powers Act (2000)

Participating organisations may grant exception to this policy if there is a genuine business requirement, but this may only be granted after an assessment, in accordance with their Risk Management Strategy, and with approval of an appropriate executive director in agreement with the director responsible for IT Services. (As defined in the CITS SLA)

This policy applies to all individuals whether directly employed by the organisation or contractors, third party service providers and private sector care providers.

Wilful or negligent disregard of this policy will be investigated and dealt with under the participating organisations' Disciplinary Procedure.

2. DEFINITIONS

Word/Term	Descriptor
Senior Information Risk Owner (SIRO)	An executive who is familiar with and takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board.
Digital & Chief Information Officer	Executive role within GHT with SIRO responsibilities
Information Assets (IAs)	Identifiable and definable assets owned or contracted by an organisation, which are valuable to the business of the organisation. These include: ▪ Information – databases, system documents and procedures, archive media/data ▪ Software – application programs, systems, development tools and utilities ▪ Physical – infrastructure, equipment, furniture and accommodation used for data processing ▪ Services – computing and communications, heating, lighting, power, air conditioning used for data processing ▪ People – their qualifications, skills and experience in use of information systems ▪ Less tangible elements – these can include the reputation and image of the organisation

Information Asset Owner (IAO)	Senior individuals involved in running the relevant business. Their role includes understanding, documenting and addressing security risks affecting the information assets they own, and providing assurance to the SIRO on the security and use of those assets
Information Governance Forensic Readiness	The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence within the law whilst minimizing the disruption or cost in doing so
IT Security Incident	Any breach or potential breach under investigation of IT information security, physical or computer related

3. POLICY STATEMENT

The main objective of this policy is 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 NHS Data Security and Protection Toolkit.

The Trust is committed to achieving and maintaining Cyber Essentials Plus Certification.

This policy applies the key concepts of Information Assurance to electronic data processing in the Trust; namely,

- Confidentiality
- Integrity
- Availability
- Accountability

4. ROLES AND RESPONSIBILITIES

Post/Group	Details
All Staff	• Accountable for the function they perform using IT equipment • Undertake mandatory training in Information Governance and Information Security • Abide by the principle of the GDPR and the Data Protection Act and other relevant legislation and information • Ensure familiarity with Trust IT security measures and that these are properly maintained • Promote a culture that values the Confidentiality, Integrity and Availability of Trust IT information assets
Department Managers	• Ensure that departmental IT processes are up to date and regularly reviewed • Ensure that departmental risk registers are regularly reviewed and acted upon • Communicate changes to IT security policy/best practice to department Line Managers • Ensure that departmental mandatory training is completed to required standards
Line Managers	• Ensure that staff are provided with the correct IT equipment and training to perform their roles in a safe and secure manner • Regularly review staff compliance with training, certification, applicable legislation • Communicate changes in policy/best practice to staff • Log and report security incidents, escalate as appropriate • Encourage staff to adopt an open approach to reporting information security incidents
Information Asset Owners (IAOs)	• Understand what information is held on their assets • Understand how information is added to, moved within and removed from their assets • Understand who/which systems have access to the information asset and ensure that use is monitored • Understand and assess the risks to Confidentiality, Availability and Integrity to information held on their assets and escalate in line with Trust Risk Management policy • Ensure that information assets, including all security risk and compliance requirements are recorded in the Organisation's information asset register • Provide written input to the Senior Information Risk Owner on the security and use of assets under their control (annually) • Ensuring information is used within the law
Information Asset Administrators (IAAs) or System Administrators	• Control access to the asset for which they are responsible • Ensure the delivery of appropriate training to users of the asset • Ensure processes are properly documented and available for dissemination to all relevant users • Record and act upon security incidents

	• Ensure the integrity of information held or processed • Agree change control processes relating to the system
IT Service Providers (CITS and third party providers)	• Responsible for the compliance of their services with this policy • Demonstrate robust processes for the identification & mitigation of IT risk • Understand the information risks and support each Organisation's response • Ensure that the Organisation is kept up to date and briefed on all information risk issues • Support the Organisation's approach to IT risk through effective resource, commitment and execution of the SLA and / or contractual obligations. • Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation in accordance with the Organisation's requirements
Digital & Chief Information Officer (SIRO)	• Understand the information risks and lead the Organisation's response • Ensure that the Board and the Accountable Officer are kept up to date and briefed on all information risk issues affecting the organisation and its business partners • Ensure that the Organisation's approach to IT risk is effective in terms of resource, commitment and execution • Own the assessment processes for information risk • Ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the Organisation • Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation, and that perceived or actual IT incidents are managed in accordance with NHS IG requirements • Provide input into the management of Serious Untoward Incidents (SUIs) relating to the information of the Organisation • Provide leadership for Information Asset Owners (IAOs) of the Organisation through effective networking structures, sharing of relevant experience/industry best practice, provision of training and creation of information risk reporting structures
Associate Chief Information Officer , IG and Health Records	• Responsible for information assurance within the Trust as such aspects as interrelate with this policy • Maintenance and review of this policy in line with legislation and national guidelines
Head of Countywide IT Services	• Accountable for the compliance of the Trust's IT services with this policy, and for the development of subsidiary policies and procedures relating to the use and management of the Trust's IT infrastructure
IT Cyber Security Team	• Responsible for identifying vulnerabilities, device configurations and software requirements that the Trust may require in order to comply with this policy, and Information • Governance and Security policies and standards
Data Protection Officer	• 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

5. THE NEED FOR IT SECURITY

With increased public awareness and reliance technology to deliver care, cyber security is an area of the organisation's operations that requires a robust approach and control. Without information the organisation could not function, so valuing and protecting the organisation's information and Information assets are crucial tasks.

Security is everybody's business and therefore everyone has a responsibility to ensure information is appropriate, secure, confidential, accurate and available only to authorised users. Without effective security, Information Assets may become unavailable, unreliable and untrustworthy, or may be compromised and used by unauthorised third parties

This policy documents requirements for the incorporation of information security practices into the daily usage of IT systems, to help ensure that patient care is not impacted through a data security breach and that the organisation is not exposed to legal, financial and governance risks from the use of electronic health care systems, electronic communications and the internet, and that its reputation is not adversely affected.

Violation of this policy may result in adverse impact on patient care, damage to the organisation's reputation, significant financial penalties, and disciplinary action up to and including dismissal.

6. IT SECURITY MANAGEMENT STRATEGIES

6.1 Risk Assessment

It is the responsibility of the IAOs and information governance teams within each Organisation to carry out local risk assessments.

The risk assessment will identify the appropriate countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

The information gained from risk assessments will be used to develop risk management strategies and processes to ensure that IT security risks are mitigated wherever possible (see 6.2 below).

Where risks cannot be mitigated, the risk should be entered on to the organisation's risk register in line with individual organisation's process and details shared with the ICS countywide cyber security team.

6.2 Management of IT Security Risks

The SIRO is accountable for ensuring that all IT security risks are managed as far as is reasonably practicable. The risk management strategies used include:

- **Appointing named individuals** to undertake defined roles relating to IT security and information governance. See the individuals identified in section 'ROLES AND RESPONSIBILITIES' section, above.
- **Applying robust access controls** to protect the information processed and stored in IT and physical systems. These measures are applied to protect the confidentiality and integrity of data held, and also to ensure compliance with legislation such as the UK GDPR and Data Protection Act
- Ensuring there are robust security requirements for **setting up user accounts, enabling user access and ensuring the user is properly authenticated** to access IT systems. This measure will also mitigate the risk of unauthorised access of information; establish user accountability and rules for access. This will also include clear policy guidance on the registration and deregistration of staff requesting access to IT facilities
- Defining a **password management policy** which stipulates the need for "strong passwords" and the management controls to ensure passwords are protected
- Ensuring that the use of all **mobile devices, removable media and "bring your own" devices** are appropriately controlled, including the use of encrypted devices where any Person Identifiable Data is used or stored on one of these devices as reflected in the organisational BYOD or portable devices policies.
- Ensuring a robust **security incident management plan** is enacted. Damage to the organisation from IT security incidents can be minimised by monitoring and acting upon them effectively
- Ensuring that the Senior responsible officer (SRO) for projects and others who implement systems include **effective security countermeasures as part of the specification and implementation as part of any new systems project**. This will include the completion of a Data protection impact assessment (DPIA). Where something is designated as an information asset, it is added to the information asset register and an asset owner is assigned.
- Ensuring that all IT **information systems, applications and networks are approved by the organisation's digital leadership before they commence operation**. Also, to ensure that information systems do not pose an unacceptable security risk to the organisation. All Digital Technology providers must record risk associated with their systems; IAOs will receive risks as part of The Digital Technology Assessment Criteria for health and social care (DTAC) and ensure mitigation is in place
- Ensuring that there is a standard operational procedure (SOP) for the **purchase and disposal of IT equipment and media** which meets the organisational IT security policy requirements
- Ensuring that there are appropriate **physical security measures** to protect IT equipment
- Ensuring the production and maintenance of **comprehensive policies and procedures** relating to all of the above, which are clear and available to all users.

- Providing Information Governance **mandatory training** to all staff relating to Data Security and Data protection
- Maintaining an information asset register which identifies the data held within an asset, the lawful basis for holding access and other security controls, associated information flows, and processing records required by UK GDPR Article 30
- Ensuring that there is a system level security control documented for an asset. This shall be mandatory for any asset identified as business critical.
- Ensuring that there are BCP and DR processes in place for all business-critical systems
- Meeting the requirements of CareCERT and protecting web applications against OWASP flagged vulnerabilities
- Meeting the National Data Guardian's Security standards

6.3 Local management of IT security risks

Information Asset Owners, Information Asset Administrators and Systems Managers are responsible for ensuring the following:

- That there are clear and robust local procedures relating to the operation of the systems under their control, to include user access controls and access rights
- That local procedures are developed in response to risk assessments
- That assets are recorded in the information asset register and reviewed at least annually

6.4 Forensic readiness

An Information Governance Forensic Readiness Policy is in place to maximise the potential to use digital evidence whilst minimising the cost of investigation by actively collecting potential evidence.

7. TRAINING

All GHT staff are informed via the Code of Confidentiality and annual Data Protection Awareness Training that they are required to have an awareness of this policy and its related documents. All partner organisation are required to ensure training compliance in line with DSPT requirements as part of CITS SLA.

8. MONITORING OF COMPLIANCE

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
Compliance with policy by all staff via audit and DSP Toolkit return, coordinated by organisation IG/IT leads	Annual	Recommendations from Cyber security operational group will be presented to The Digital Care Delivery Group (DCDG)
Exception monitoring of Datix Web reports by Trust IG/IT leads	Bi-monthly	Monitored by IG Core Group, issues reported to the IG and HR Operational Group
Monitoring of breaches reported to the IT Service Desk by service desk leads	Ongoing	Reviewed by IT Security Officer, escalated to IG/IT leads. Further escalation via IT Security Panel.

9. REFERENCES

Cyber Essentials	National Cyber Security Centre
Digital Social Care Security Standards	National Data Guardian

DOCUMENT PROFILE	
Reference Number	B0591
Title	IT Security
Category	Non-Clinical
Version	V5
Issue Date	July 2023
Review Date	July 2026
Owning Division	Corporate
Owning Specialty	Information Governance
Associated Specialities	Cyber Security, IT
For Use By	GHNHST & GMS STAFF (Shared with ICS partner organisations for adoption as part of CITS SLA)
Author	Thelma Turner Associate CIO IG and Health Records
Quality Assurance Group	DCDG
Other Approving Groups	IGHR Operational Group ICS Cyber Security Group Digital and Information Senior Leads
Local Approval Details	DCDG 06/06/2023
TPAG Ratification	July 2023
Consultees	IGHR Operational Group ICS Cyber Security Group Digital and Information Senior Leads CITS Operational Team Leads
Dissemination Details	Upload to Policy Site; global email; copy of policy will be issued to all staff authorised to use IT systems within the Trust. Updated guidance and specific security alerts will be issued by global or targeted communications from IT Services or Information Governance on an ad hoc basis
Keywords	Security, IT, risk assessment
Equality Impact Assessment (EIA)	B0591 EIA
Related Trust Documents	AC1 - IT Access Control AC2 - Registration and de-registration AC3 - Password usage and management AC4 - Physical and environmental security AC5 - Purchase and disposal of equipment
Other Relevant Documents	Disciplinary Procedure; Information Governance Policy;
External Compliance Standards and/or Legislation	The Data Protection Act 2018 UK General Data Protection Regulation Computer Misuse Act 1990 Copyright Designs & Patents Act 1988 Regulation of Investigatory Powers Act 2000