Policy

TETBURY HOSPITAL

IT SECURITY POLICY

Department / Service:	All
Originator:	Countywide IT Services Gloucestershire
Accountable Director:	Chief Executive Officer
Approved by:	IG & Records Management Committee
Date of approval:	
Revision Due:	2021
Target Organisation(s)	Tetbury Hospital Trust Ltd
Target Departments	All
Target staff categories	All

Policy Overview:

This document defines the recommended IT Security Policy for 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. 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. This policy will not be adapted to Tetbury Hospital IT structure.

Key amendments to this Document:

Date	Amendment	By:
3/15	Adopted from Countywide IT Services	JJ
11/18	First revision/update to GDPR	JJ

Gloucestershire Hospitals NHS

TRUST POLICY

IT SECURITY

Any hard copy of this document is only assured to be accurate on the date printed. The most up to date version is available on the Trust Policy Site.

All document profile details are recorded on the last page.

All documents must be reviewed by the last day of the month shown under “review date”, or before this if changes occur in the meantime.

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

IT SECURITY

Gloucestershire Hospitals NHS

NHS Foundation Trust

IT SECURITY POLICY

1. INTRODUCTION

This document defines the recommended IT Security Policy for 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. 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 development, operation and use of the Trust's IT infrastructure

Read this document in conjunction with the Information Governance policy. The legal framework for this policy includes:

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

The Trust may grant exception to this policy if there is a genuine business requirement, but this may only be granted after an assessment and with approval of an appropriate executive director in agreement with the director responsible for IT Services.

This policy applies to all individuals who access or process data held by the Trust, whether directly employed by the Trust 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 Trust 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
Chief Information Officer (CIO)	Senior manager responsible for managing and escalating information risk

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 is to understand and address risks to the information assets they own, and to provide 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 maximize 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 of information/security, physical or computer related

3. PURPOSE

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 unauthorized 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 Connecting for Health Information Governance Toolkit.

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 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 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	▪ 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
	▪ Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation in accordance with the Organisation's requirements ▪ Provide support for Information Asset Owners (IAOs) of the Organisation through effective IT support
Chief Information Officer (CIO) and Senior Information Risk Owner (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
Information Governance Manager	▪ Responsible for information assurance within the Trust as such aspects as interrelate with this policy ▪ 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 ▪ Maintenance and review of this policy in line with legislation and national guidelines
IT Security Officer	▪ Responsible for identifying 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

5. THE NEED FOR IT SECURITY

With increased public awareness of identity theft and the power of information, information security is the area of the Trust's operations that most needs control. Without information the Trust could not function, so valuing and protecting the Trust's information 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 authorized users. Without effective security, Trust Information Assets may become unreliable and untrustworthy, may not be accessible where or when needed or may be compromised by unauthorized third parties

This policy sets forth requirements for the incorporation of information security practices into the daily usage of Trust systems, to help ensure that the Trust is not exposed to legal and governance risks from the use of electronic communications and the internet, and that its reputation is not adversely affected.

Violation of this policy may result in damage to the Trust'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 of 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 organisational risk managers are responsible for ensuring that these are entered on to the Trust's risk register.

6.2 Trustwide management of IT security risks

The organisational IG managers are responsible for ensuring that all IT security risks are managed as far as is reasonably practicable. The risk management strategies used includes:

- **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 Trust IT systems. These measures are applied to protect the confidentiality and integrity of data held, and also to ensure compliance with legislation such as the 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 Trust IT systems. This measure will also mitigate the risk of unauthorized 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 Trust 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
- Ensuring a robust **security incident management procedure** is enacted. Damage to the Trust from IT security incidents can be minimized by monitoring and acting upon them effectively
- Ensuring that Project Managers 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 privacy impact assessment. Identification of an information asset owner and registration as an asset on the Trust's information asset register
- Ensuring that all **information systems, applications and networks are approved by the director responsible for IT services before they commence operation**. Also to ensure that information systems do not pose an unacceptable security risk to the organisation. Clinical systems providers must record risk associated with their systems; IAOs will receive risks and ensure mitigation is in place
- Ensuring that the **purchase and disposal of IT equipment and media** is appropriately controlled to protect information assets
- Ensuring that there are appropriate **security measures** to protect Trust-owned IT equipment
- Ensuring the production and maintenance of **comprehensive policies and procedures** relating to all of the above, which are clear and disseminated to all relevant users. These are listed in the
- Providing **mandatory training** to all staff in Information Governance and IT Security

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

6.4 Forensic readiness

The Trust has approved the introduction of Information Governance (IG) forensic readiness into its business processes and functions; in order to maximize the potential to use digital evidence whilst minimizing the cost of investigation by actively collecting potential evidence. This evidence may be collected in advance of a crime or incident and will be used to the benefit of the organisation, its patients and staff. For example, the Trust may employ logging software to determine detailed user and machine interactions with files stored on the network, which might include details of when files are accessed and by whom, when/if they are transferred off the network and/or shared with other users, when they are moved to another network storage location and when/if they are deleted. This decision reflects the high level of importance placed upon minimizing the impacts of information security events.

7. TRAINING

All users are required to have an awareness of this policy and its related documents.

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 Data Security & Protection Toolkit coordinated by Trust IG/IT leads	Annual	• Recommendations from IT Security Panel will be presented to IM&T Board
• 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 Specialist 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.

IT SECURITY – DOCUMENT PROFILE

DOCUMENT PROFILE	
REFERENCE NUMBER	B0591
CATEGORY	Non-Clinical
VERSION	V3
SPONSOR	Zack Pandor, Director of CITS
AUTHOR	Rob Holmes, IT Security Officer (technical authoring support, Kym Ypres-Smith)
ISSUE DATE	January 2015
REVIEW DETAILS	January 2018 – review by Director of IT
ASSURING GROUP	Trust Policy Approval Group
APPROVING GROUP	IG and HR Committee
APPROVAL DETAILS	Policy approval: IG and HR Committee, September 2014 TPAG approval: 16th December 2014
CONSULTEES	Countywide IT Security Panel
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
RELATED TRUST DOCUMENTS	Action cards ITS1 – ITS6; IT Security Document Matrix
OTHER RELEVANT DOCUMENTS	Trust Disciplinary Procedure; Information Governance Policy;
EXTERNAL COMPLIANCE STANDARDS AND/OR LEGISLATION	• The Data Protection Act (1998) • Computer Misuse Act (1990) • Copyright Designs & Patents Act (1988) • Regulation of Investigatory Powers Act (2000)

9. Appendix 1 – User Access

Access controls exist to protect the information processed and stored in IT systems. They are applied to protect the confidentiality and integrity of data held by the Trust and to help the trust comply with legislation such as the Data Protection Act. Access will be granted on the principle of **least privilege**. This means that members of staff will be provided access rights only to the level that they require in order to carry out their legitimate Trust business activities

Controls:
IT systems are subject to the following management controls:

Director of IT Services

Responsible for overall IT security, defining the organisation's standards for access controls (usually a user name and password) and remote access

Head of Information Governance

Responsible for the Trust's register of Information Assets and records of third party and/or remote access

Information Asset Owners

Managing all risks associated with the systems under the control and implementing effective system level access controls

Information Asset Administrator

Manage day-to-day creation, modification and deletion of access control entries.
Ensure that new users are appropriately authorised, and adopt processes for reviewing and revoking access rights where required

Line managers

Request access levels for staff groups within their area, and maintaining appropriate records

All staff

Ensure their own system access details are kept secure and used in accordance with the Trust's business

General guidance:

• All access to systems must be authorised by its Information Asset Owner – At Tetbury Hospital Trust, Head of Information, IT & Admin authorises access to IT systems.

• Access to systems is not permitted when authorisation has expired (e.g. at the end of a project, or when an employee leaves the Trust). This applies even if accounts, access rules or access tokens have remained in place.

• Any individual who discovers (intentionally or unintentionally) a means to bypass system access controls must report this promptly to their line manager or IT. Intentional abuse of access controls constitute a serious disciplinary offence and could also result in legal action.

• Systems will be tested for resilience by competent persons under controlled conditions.

• Users shall sign on with the least level of system privilege required for the particular task at hand.

• "Super-user" privileges must only be used when actually needed

- Users must not share their username or password (see action card ITS3) with anyone else, including IT support staff, or leave accounts logged in when they are away from a terminal
- Third party users must be specifically authorised by the Information Asset Owner and the Head of Information Governance

IT System restrictions:

- There is no direct write access to any PC and/or server
- All software applications must be installed by IT (Countywide IT Services for secure link PC's)
- All access to another user's files must be authorised by a senior manager or director before access can be given by IT
- High level system privileges will only be authorised where there is a specific requirement

Guidance for Application Administrators:

All application administrators must:

- Control user access to information and system functions according to a defined system level access control policy
- Prevent unauthorised access to any utility or system function that can override access controls
- Protect the security of other systems with which information and resources are shared
- Provide an audit function to enable the monitoring of successful and unsuccessful access to the system and the data contained therein.

Login warnings:

Warnings will be displayed on system login banners which shall say:

- The system is for authorised users only
- Usage is monitored
- Evidence of misuse may result in legal proceedings

10. APPENDIX 2 – REGISTRATION/DE-REGISTRATION

This outlines the process for registration to the secure IT system and also for the Tetbury Hospital Private system.

When a new employee joins the team, the line manager will determine what access is required.
All new starters will be required to complete a General network use form found in the recruitment folder. The access required should be discussed with the Head of Information, Technology & Administration, who will be required to authorise this.

An nhs.net email account will be issues only if required to be able to carry out the job role. Access to software such as Trak, PACS, ICE should be arranged through the Head of Information Technology.

The general network use form should be scanned and sent to IT service desk and Countywide IT Services for processing.

In order for relevant training of the Trak system, an E-learning account will be set up.

For Tetbury Private System – a personal email will be issued by the Head of Information, Technology & Administration through Office 365. Staff will be granted access to those folders that are pertinent to their job role.

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the policy/guidance affect any one group less or more favourably than another on the basis of:**		
	• Age	No	
	• Disability	No	
	• Gender reassignment	No	
	• Gender	No	
	• Race	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Marriage and Civil Partnership	No	
	• Pregnancy and Maternity	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	NA	
4.	**Is the impact of the policy/guidance likely to be negative?**	NA	
5.	**If so can the impact be avoided?**	NA	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	NA	
7.	**Can we reduce the impact by taking different action?**	NA	

Supporting Document 2 – Financial Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	**Yes/No**
1.	Does the implementation of this document require any additional Capital resources	
2.	Does the implementation of this document require additional revenue	
3.	Does the implementation of this document require additional manpower	
4.	Does the implementation of this document release any manpower costs through a change in practice	
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	
	Other comments:	

Supporting Document 3 – Data Protection Impact Assessment

Please review the question below: Answering ‘yes’ to any of these questions is an indication that a DPIA is required

	Title of document:	**Yes/No**
1.	Will the policy involve systematic and extensive profiling or automated decision-making to make significant decisions about people	Y/N
2.	Will the policy process special category data or criminal offence data on a large scale	Y/N
3.	Systematically monitor a publicly accessible place on a large scale	N
4.	Use new technologies	N
5.	Use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit	N
6.	Carry out profiling on a large scale	N
7.	Process biometric or genetic data	N
8.	Combine, compare or match data from multiple sources	N
9.	Process personal data without providing a privacy notice directly to the individual	
10.	Process personal data in a way which involves tracking individuals online or offline location or behaviour	
11	Process children’s personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	
12	Process personal data which could result in a risk or physical harm in the event of a security breach	
13	Systematic processing of sensitive data or data of a highly personal nature	
14	Processing on a large scale	
15	Processing of data concerning vulnerable data subjects	
16	Innovative technological or organisational solutions	
17	Processing involving preventing data subjects from exercising a right or using a service or contract	

	Title of document:	Yes/No
18	Is this a major project involving the use of personal data	
	Comments: **If we decide not to carry out a DPIA we document our reasons why** **We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing**	