

## 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.

#### FAST FIND:

This policy works in conjunction with a large number of related documents. See [the IT Security Policy Document Matrix and Quick Guide](#) for a detailed overview.

#### See also:

- [Action card ITS1 – IT Access Control](#)
- [Action card ITS2 – Registration and de-registration](#)
- [Action card ITS3 – Password usage and management](#)
- [Action card ITS4 – Physical and environmental security](#)
- [Action card ITS5 – Purchase and disposal of equipment](#)
- [Action card ITS6 – Fax protocol](#)

#### DOCUMENT 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 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

1. INTRODUCTION
2. DEFINITIONS
3. PURPOSE
4. ROLES AND RESPONSIBILITIES
5. THE NEED FOR IT SECURITY
6. IT SECURITY MANAGEMENT STRATEGIES
7. TRAINING
8. MONITORING OF COMPLIANCE

### Action cards

[ITS1](#)

[ITS2](#)

[ITS3](#)

[ITS4](#)

[ITS5](#)

[ITS6](#)

[IT Access Control](#)

[Registration and De-registration](#)

[Password Usage and Management](#)

[Physical and Environmental Security](#)

[Purchase and Disposal of IT Equipment](#)

[Fax protocol](#)

## 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 – see the [IT Security Policy Document Matrix and Quick Guide](#).

Read this document in conjunction with the [Information Governance policy](#). The legal framework for this policy includes:

- The Data Protection Act (1998)
- 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.

Willful or negligent disregard of this policy will be investigated and dealt with under the [Trust Disciplinary Procedure](#).

### 2. DEFINITIONS

Word/Term	Descriptor
<b>Senior Information Risk Owner (SIRO)</b>	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
<b>Chief Information Officer (CIO)</b>	Senior manager responsible for managing and escalating information risk
<b>Information Assets (IAs)</b>	Identifiable and definable assets owned or contracted by an organisation, which are valuable to the business of the organisation. These include: <ul style="list-style-type: none"> <li>▪ Information – databases, system documents and procedures, archive media/data</li> <li>▪ Software – application programs, systems, development tools and utilities</li> <li>▪ Physical – infrastructure, equipment, furniture and accommodation used for data processing</li> <li>▪ Services – computing and communications, heating, lighting, power, air conditioning used for data processing</li> <li>▪ People – their qualifications, skills and experience in use of information systems</li> <li>▪ Less tangible elements – these can include the reputation and image of the organisation</li> </ul>
<b>Information Asset Owner (IAO)</b>	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
<b>Information Governance Forensic Readiness</b>	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
<b>IT Security Incident</b>	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
<b>All Staff</b>	<ul style="list-style-type: none"> <li>▪ Accountable for the function they perform using IT equipment</li> <li>▪ Undertake mandatory training in Information Governance and Information Security</li> <li>▪ Abide by the principle of the Data Protection Act and other relevant legislation and information</li> <li>▪ Ensure familiarity with Trust IT security measures and that these are properly maintained</li> <li>▪ Promote a culture that values the Confidentiality, Integrity and Availability of Trust IT information assets</li> </ul>
<b>Department Managers</b>	<ul style="list-style-type: none"> <li>▪ Ensure that departmental IT processes are up to date and regularly reviewed</li> <li>▪ Ensure that departmental risk registers are regularly reviewed and acted upon</li> <li>▪ Communicate changes to IT security policy/best practice to department Line Managers</li> <li>▪ Ensure that departmental mandatory training is completed to required standards</li> </ul>
<b>Line Managers</b>	<ul style="list-style-type: none"> <li>▪ Ensure that staff are provided with the correct IT equipment and training to perform their roles in a safe and secure manner</li> <li>▪ Regularly review staff compliance with training, certification, applicable legislation</li> <li>▪ Communicate changes in policy/best practice to staff</li> <li>▪ Log and report security incidents, escalate as appropriate</li> <li>▪ Encourage staff to adopt an open approach to reporting information security incidents</li> </ul>
<b>Information Asset Owners (IAOs)</b>	<ul style="list-style-type: none"> <li>▪ Understand what information is held on their assets</li> <li>▪ Understand how information is added to, moved within and removed from their assets</li> <li>▪ Understand who/which systems have access to the information asset and ensure that use is monitored</li> <li>▪ 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</li> <li>▪ Ensure that information assets are recorded in the Organisation's information asset register</li> <li>▪ Provide written input to the Senior Information Risk Owner on the security and use of assets under their control (annually)</li> <li>▪ Ensuring information is used within the law</li> </ul>
<b>Information Asset Administrators (IAAs) or System Administrators</b>	<ul style="list-style-type: none"> <li>▪ Control access to the asset for which they are responsible</li> <li>▪ Ensure the delivery of appropriate training to users of the asset</li> <li>▪ Ensure processes are properly documented and available for dissemination to all relevant users</li> <li>▪ Record and act upon security incidents</li> <li>▪ Ensure the integrity of information held or processed</li> <li>▪ Agree change control processes relating to the system</li> </ul>
<b>IT Service Providers</b>	<ul style="list-style-type: none"> <li>▪ Responsible for the compliance of their services with this policy</li> <li>▪ Demonstrate robust processes for the identification &amp; mitigation of IT risk</li> <li>▪ Understand the information risks and support each Organisation's response</li> <li>▪ Ensure that the Organisation is kept up to date and briefed on all information risk issues</li> <li>▪ Support the Organisation's approach to IT risk through effective resource, commitment and execution of the SLA</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Ensure that identified IT threats and vulnerabilities are followed up for risk mitigation in accordance with the Organisation's requirements</li> <li>▪ Provide support for Information Asset Owners (IAOs) of the Organisation through effective IT support</li> </ul>
<b>Chief Information Officer (CIO) and Senior Information Risk Owner (SIRO)</b>	<ul style="list-style-type: none"> <li>▪ Understand the information risks and lead the Organisation's response</li> <li>▪ 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</li> <li>▪ Ensure that the Organisation's approach to IT risk is effective in terms of resource, commitment and execution</li> <li>▪ Own the assessment processes for information risk</li> <li>▪ Ensure that there are effective mechanisms in place for reporting and managing Serious Untoward Incidents (SUIs) relating to the information of the Organisation</li> <li>▪ 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</li> <li>▪ Provide input into the management of Serious Untoward Incidents (SUIs) relating to the information of the Organisation</li> <li>▪ 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</li> </ul>
<b>Information Governance Manager</b>	<ul style="list-style-type: none"> <li>▪ Responsible for information assurance within the Trust as such aspects as interrelate with this policy</li> <li>▪ 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</li> <li>▪ Maintenance and review of this policy in line with legislation and national guidelines</li> </ul>
<b>IT Security Officer</b>	<ul style="list-style-type: none"> <li>▪ 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</li> </ul>

## 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 [IT Security Policy Document Matrix and Quick Guide](#).
- 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?	<b>YES</b>
--	------------

<b>Monitoring requirements and methodology</b>	<b>Frequency</b>	<b>Further actions</b>
<ul style="list-style-type: none"> <li>Compliance with policy by all staff via audit and IG Toolkit return, co-ordinated by Trust IG/IT leads</li> </ul>	Annual	<ul style="list-style-type: none"> <li>Recommendations from IT Security Panel will be presented to IM&amp;T Board</li> </ul>
<ul style="list-style-type: none"> <li>Exception monitoring of Datix Web reports by Trust IG/IT leads</li> </ul>	Bi-monthly	<ul style="list-style-type: none"> <li>Monitored by IG Core Group, issues reported to the IG and HR Specialist Group</li> </ul>
<ul style="list-style-type: none"> <li>Monitoring of breaches reported to the IT Service Desk by service desk leads</li> </ul>	Ongoing	<ul style="list-style-type: none"> <li>Reviewed by IT Security Officer, escalated to IG/IT leads. Further escalation via IT Security Panel.</li> </ul>

## IT SECURITY – DOCUMENT PROFILE

<b>DOCUMENT PROFILE</b>	
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: 16 <sup>th</sup> 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 <a href="#">ITS1 – ITS6</a> ; <a href="#">IT Security Document Matrix</a>
OTHER RELEVANT DOCUMENTS	<a href="#">Trust Disciplinary Procedure</a> ; <a href="#">Information Governance Policy</a> ;
EXTERNAL COMPLIANCE STANDARDS AND/OR LEGISLATION	<ul style="list-style-type: none"> <li>• The Data Protection Act (1998)</li> <li>• Computer Misuse Act (1990)</li> <li>• Copyright Designs &amp; Patents Act (1988)</li> <li>• Regulation of Investigatory Powers Act (2000)</li> </ul>