WHICTS Policy	

Information Security Policy

Department / Service:	IM&T	
Originator:	Ruth King	ICT Security Manager
Accountable Director:	Jonathan Rex	Interim Director of ICT
Approved by:	County and Organisation IG Steering Groups and their relevant processes	
Date of approval:	25th September 2013	
First Revision Due:	25th September 2015	
Target Organisation(s)	Worcestershire Local Health Community and all users of the WHICTS Network	
Target Departments	All	
Target staff categories	All	

Policy Overview
This policy is aimed at providing a comprehensive and consistent approach to the security management of information across the Worcestershire Local Health Community in line with the DH Information Security Management: NHS Code of Practice (April 2007). The purpose of the policy is to provide a balance between security and ease of use, and to take full account of NHS guidance and legislation.

Key amendments to this Document:

Date	Amendment	By:
Jan 2011	Policy based on CfH template; replacing previous Nov 2007 policy	R King
Jan 2013	Two yearly review; minor updates, including format update	R King
July 2013	Monitoring table added	R King
August 2013	Term Trust changed to Organisation	R King

Contents page:

Appendices

1. Introduction

This top-level information security policy is a key component of Worcestershire NHS community overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. This policy is aimed at providing a comprehensive and consistent approach to the security management of information across the Worcestershire NHS community in line with the DH Information Security Management: NHS Code of Practice (April 2007). It will ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.
If any user disregards the rules set out in this Information Security Policy, the user will be fully liable and may be subject to disciplinary action by their employing Organisation.

2 Scope of this document

2.1 Scope

This policy applies to all full time and part time employees, non-executive directors, contracted third parties (including agency staff), students/trainees and other staff on placement and includes the use of mobile devices.

2.2 Policy Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WHICTS:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the Organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the Organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the Organisation.

2.3 Objectives

The objectives of Worcestershire Health ICT Services (WHICTS) Information Security Policy are to preserve:

- **Confidentiality** - Access to Data is confined to those who have legitimate authority to view it.
- **Integrity** – Data is timely and accurate and detected or amended only by those specifically authorised to do so.

- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

3 Definitions

DH	Department of Health
HSCIC	Health & Social Care Information Centre
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICT	Information & Communication Technology
IG	Information Governance
IGSG	Information Governance Steering Group
IGT	Information Governance Toolkit
IGTT	Information Governance Training Tool
IM&T	Information Management & Technology
IT	Information Technology
NHS	National Health Service
NHSCFS	NHS Counter Fraud Services
PC	Personal Computer
PID	Person Identifiable Data
RA	Registration Authority
SIC	Statement of Internal Control
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
SLSP	System Level Security Policies
WHICTS	Worcestershire Health Information & Communication Technology Services

4 Responsibilities and Duties

4.1 Chief Executive

Information security is the responsibility of all staff within the Worcestershire Organisations. Ultimate responsibility for information security resides with each Organisation's Chief Executive. This responsibility should be discharged through a designated senior member of staff who has lead responsibility.

4.2 Director of ICT

The Director of ICT has been delegated with responsibility for information security on behalf of the Chief Executives. The day to day activities required to effectively implement and maintain this policy with be performed through the Countywide Information Security Manager.

4.3 Senior Information Risk Owner (SIRO)

The Organisation's SIRO is accountable for fostering a culture for protecting and using data, providing a focal point for managing information risks and incidents and is concerned with the management of all information assets.

4.4 Information Asset Owner (IAO)

The Organisation's IAO's role is to understand and address risks to the information assets they 'own'; and provide assurance to the SIRO on the security and use of these assets.

4.5 Information Asset Administrator (IAA)

The Organisation's IAA will provide support to their IAO by: ensuring that policies and procedures are followed, recognising potential or actual security incidents, consulting their IAO on incident management and ensuring that information asset registers are accurate and maintained up to date

4.6 Caldicott Guardian

The Organisation's Caldicott Guardian has a strategic role in ensuring that there is an integrated approach to information governance, developing security and confidentiality policy and representing confidentiality requirements and issues at Board level.

4.7 Information Security Manager

The Countywide Information Security Manager is responsible for the implementation and enforcement of the Information Security policy.
Responsibilities include:

- Ensuring that policies, procedures and working practices align themselves to this information security policy.
- Monitoring and reporting on the status of IT security within the Organisations.
- Ensuring compliance with relevant legislation and regulation.
- Ensuring that staff are aware of their responsibilities and accountability within information security
- Monitoring for potential security breaches.
- Working closely with those responsible for Freedom of Information, Data Protection, patient confidentiality and other Information Governance work areas.
- Ensuring that risk assessments are carried out along with any associated improvement plans.
- Providing direct input to the information security components of the IG Toolkit.

4.8 Information Governance Leads

In addition to the Information Security Manager, each Organisation has an Information Governance lead responsible for:

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance

- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance.

In addition there exists a Countywide Information Governance Steering Group which comprises the Organisations Information Governance leads and the Information Security Manager. Through this group common approaches are agreed to aspects of Information Governance where appropriate. Together they have joint responsibility for completion of the IG Toolkit.

4.9 Directors and Departmental Managers

Directors and departmental managers must ensure:

- They are kept appraised of all information security and governance guidance
- That all staff are aware of their security responsibilities
- That staff have appropriate training for the systems they are using
- That appropriate levels of access are granted to specific individuals (e.g. Registration Authority role for staff who issue smartcards)
- Ensure that all staff sign confidentiality agreements as part of their contract of employment
- Ensure that IT, RA and system managers are informed of staff role changes, new starters and leavers.
- The security of physical environments where information is processed or stored

4.10 System Managers

An IAO will be designated for each information system within the Organisation. The IAA will be responsible for the day to day management of that system; including a system specific Information Security Policy, Information Asset Registration and Risk Assessment. The IAA will ensure that the Information Security Policy and associated procedures are enforced within their areas of responsibility.

4.11 Individual staff

All staff, including contract and temporary workers are:

- Responsible for conformance to the information security policy and associated guidelines and best practice.
- Expected to report information security incidents to their line manager in accordance with local incident reporting procedures.
- Required to sign a general statement of confidentiality on commencement of employment.
- Required to sign the User Responsibility Statement that is contained within the Information Security Declaration (Appendix 1 of this document). This is as

an indication that they accept responsibility for maintaining security and confidentiality and that they understand the consequences of any breach.

4.12 Contractors

In addition to the responsibilities for individual staff, as detailed above, the contractor must obtain authorisation for use of their laptop on Organisation's premises. This should be obtained through the Organisation's manager they are reporting to, who will co-ordinate the request with WHICTS. Any requirement to store Organisation's data on the laptop must have been specifically authorised by the Organisation's manager, and where appropriate, if Person Identifiable Data (PID), confidential or sensitive information the Caldicott Guardian/Information Governance Manager/Information Asset Owner (IAO)/Senior Information Risk Owner (SIRO); Information Governance will be able to clarify this process further details can be found on the Connecting for Health Website. The laptop needs to be encrypted to the DH approved level; this can be verified with WHICTS.

5 Legislation

The Worcestershire NHS community is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Worcestershire NHS community, who may be held personally accountable for any breaches of information security for which they may be held responsible, failure to comply could result in the individual or the Organisation being prosecuted. The Worcestershire NHS community shall comply with the legislation, detailed in section 10, and other legislation as appropriate:

6. Policy Detail

6.1 Document Framework

Document Title	Content	Review period
Information Security Policy	Principles	2 Years
User Responsibility Declaration	Statement	2 Years
Information Security Policies & Procedures ▪ Access Control ▪ Anti-Virus ▪ Back-Up ▪ Business Continuity ▪ Equipment Disposal ▪ Internet and E-Mail Access ▪ Mobile Devices ▪ Network Security	Requirements	2 Years

Organisation Policies & Procedures ▪ Code of Conduct in Respect of Confidentiality ▪ Data Protection ▪ Disciplinary ▪ Freedom of Information ▪ Home Working ▪ Incident Reporting ▪ Information Governance ▪ Information Risk ▪ Records Management ▪ Safe Haven	Requirements	As per Organisation requirements

6.2 Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary through the IGTT

6.3 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

6.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named Information Asset Owner and Information Asset Administrator who shall be responsible for the information security of that asset.

6.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

6.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

6.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

6.8 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. This will be achieved by the effective use of suitable security measures i.e. physical controls within buildings, entry systems and secure storage facilities to protect assets from theft/damage.

6.10 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by WHICTS, specified in the Network Security Policy.

6.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis, by their IAO. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Worcestershire NHS community risk management programme. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

6.12 Information security events and weaknesses

All information security events and suspected weaknesses are to be reported via the IT Helpdesk, for the attention of the Information Security Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

6.13 Protection from Malicious Software

The Organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the Organisation's property without permission from WHICTS. Users breaching this requirement may be subject to disciplinary action.

6.14 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of WHICTS before they may be used on Organisation systems. Such media must also be fully virus

checked before being used on the Organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

6.15 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Organisation has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act

6.16 Accreditation of Information Systems

The Organisation shall ensure that all new information systems, applications and networks include an approved security plan before they commence operation.

IAOs are responsible for System Level Security Policies (SLSPs) for systems under their control in order to distinguish between the security management considerations and requirements in this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system.

6.17 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by WHICTS.

6.18 Intellectual Property Rights

The Organisation shall ensure that all information products are properly licensed and approved by WHICTS. Users shall not install software on the Organisation's property without permission from WHICTS. Users breaching this requirement may be subject to disciplinary action.

6.19 Business Continuity and Disaster Recovery Plans

The Organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

6.20 Reporting

The Information Security Manager shall keep the Countywide and individual Organisation and IG Steering Groups informed of the information security status of the Organisation by means of regular reports and presentations.

6.21 Policy Audit

This policy shall be subject to audit by CW Audit.

6.22 Further Information

Further information and advice on this policy can be obtained from the Information Security Manager.

7. Implementation

7.1 Plan for implementation

WHICTS will ensure this policy is sent to each Organisation's Information Governance Manager who will arrange for it to be communicated through their appropriate channels - including all directorate managers within the Organisation, whose responsibility it will then be to ensure that all staff groups within their area are directed to this policy.

7.2 Dissemination

This policy will be available on the Organisation Intranet. IG will arrange for the policy to be communicated through their appropriate channels.

7.3 Training and awareness

This Policy will be promoted by WHICTS including the training department and Information Security manager; each Organisation's Information Governance Team will also promote the Policy. This Policy will also be included, along with the Information Security Policy, as a requirement for any new staff member to sign up to via the User Declaration. Any key amendments to the Policy will be notified to each Organisation for communication to staff groups. Staff are also required to complete mandatory IG training via the IGTT.

8. Monitoring and Compliance

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: (Responsible for also ensuring actions are developed to address any areas of non-compliance)	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 6&12	Breaches in policy and incidents will be identified and reported.	Initially logged as a call via the Service Desk for evaluation and, where appropriate, an Incident being raised and investigated as per each Organisation's guidelines.	Whenever a breach in Policy or an incident occurs	Investigating officer	Reported in line with Organisation Policy through IG leads and IGSG; where appropriate being escalated in line with SIRI guidelines.	Low level breaches and Incidents will be reviewed at Organisation's IGSG 4 times a year. Serious incidents will also follow this process and are additionally included in the individual Organisation's SIC and annual report, in line with HSCIC SIRI guidance.

9. Policy Review

The Information Security Manager will ensure that any updates or new legislation will be reflected in this policy and disseminated throughout the Organisation if changes are made prior to the next revision of the policy, due in 24 months from approval.

10. References

Access to Health Records Act	1990
Caldicott Principles	
Care Quality Commission	
Common Law Duty of Confidentiality	
Computer Misuse Act	1990
Copyright, Designs and Patents Act	1988
Criminal Justice and Public Order Act	1994
Data Protection Act/ Processing of Sensitive Personal Data Order	1998/2000
Freedom of Information Act 2000	2000
Health and Safety at Work Act	1974
Health and Social Care Act	2012
HSCIC Information Governance Toolkit	
Human Rights Act	1998
Information Security Management: NHS Code of Practice - DH	2007
Interception Of Communications Act	1985
ISO/IEC 27001 Information Security Management Standard	
NHS Code of Practice	2006
NHS Code for Records Management	2006
Reporting, Managing and Investigating IG Serious Incidents Requiring Investigation (SIRI)	2013
Regulation of Investigatory Powers	2000
Trade Mark Act	1994

11. Background

11.1 Equality Requirements

No potential discriminatory impact has been identified as a result of the Equality Impact Assessment Tool, so not required to refer to Human Resources (Appendix 2)

11.2 Financial Risk Assessment

No business case has been completed as nothing highlighted as a result of the Financial Risk Assessment (Appendix 4).

11.3. Consultation Process

The following stakeholders have been consulted during the production of this Policy:
WHICTS
Information Governance Groups at Organisation and County level
Organisation's Counter Fraud Managers

11.4. Approval Process

As a WHICTS Policy each Organisation will co-ordinate approval via their IG Steering Groups and any additional identified committees, as detailed in the Checklist for the Review and Approval key document (Appendix 3).

Appendix 1 - Users Responsibility Statement

1.1 The purpose of this document is to summarise the key user responsibility requirements as laid out in the following documents:

- Information Security Policy
- Internet and E-Mail Access Policy
- Mobile Computing Policy
- Anti Virus Policy
- Relevant Organisation's Incident Reporting Procedure
- Access control Policy
- Safe Haven Policy
- Equipment Disposal Policy
- Home working Policy
- Code of Conduct for Employees in Respect of Confidentiality

1.2 These documents support the Organisation's overall Information Security Policy which sets out guidelines within the framework of the DH Information Security Management: NHS Code of Practice (April 2007). It is your manager's responsibility to ensure that you are aware of those policies which are relevant to your role within the Organisation.

1.3 The purpose of the Policy is to preserve:

- Confidentiality – Access to data is confined to those who have legitimate authority to view it.
- Integrity – Data is timely and accurate and detected or amended only by those specifically authorised to do so.
- Availability – Data is available to those authorised when it is needed

By following the guidelines in this statement the users can minimise risks in relation to information security. Non-compliance may result in disciplinary action being taken in accordance with relevant Organisation's disciplinary policy, and may lead in very serious cases to dismissal for gross misconduct, as detailed in your Organisation's Code of Conduct for Employees in Respect of Confidentiality.

To obtain a copy of the disciplinary policy please discuss with your manager or the Human Resources department. .

2. Safeguarding Data - IT Security Essentials

- Use your own password, ensure that it is kept secret at all times and never use somebody else's.
- Don't leave computers open for unauthorised access, ensure either logged out or locked (Ctrl+Alt+Delete) when unattended.
- Only share person identifiable data with those who are authorised to see it.
- Save all data to network drives, e.g. M drive, not to your C:\ drive as network data is secure and backed up.
- Do not hold Person Identifiable Data (PID) on portable media (including laptops) unless it is encrypted. Please contact the IT department for further guidance.
- Ensure that laptops are backed up regularly to a network drive and that they are logged onto the network regularly to receive antivirus and other major updates.
- Only send patient identifiable information, outside WHICTS, through NHSmail i.e. between email addresses that end in nhs.net. Alternatively the data must be encrypted.
- Do not use the internet inappropriately.
- Do not load unofficial software onto Organisation computers (including laptops)
- All mobile devices should be password protected and laptops should be encrypted, with WHICTS software.

3. Caldicott Principles

The Caldicott Report set out a number of general principles that health Organisations should use when reviewing its use of client information and these are set out below:

Principle 1: Justify the purpose(s)

Every proposed use or transfer of personally identifiable information within or from an Organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary.

Personally identifiable information items should not be used unless there is no alternative.

Principle 3: Use the minimum personally identifiable information.

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

Principle 4: Access to personally identifiable information should be on a strict need to know basis.

Only those individuals who need access to personally identifiable information should have access to it.

Principle 5: Everyone should be aware of their responsibilities.

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Principle 6: Understand and comply with the law.

Every use of personally identifiable information must be lawful. Someone in each Organisation should be responsible for ensuring that the Organisation complies with legal requirements.

User Responsibility Declaration

I confirm that I have read and understood the content of the Information Security Policy, the Internet and Email Access Policy and any other Policies relevant to my role. By doing this I therefore accept responsibility for maintaining security and confidentiality within my working practices.

I acknowledge that wilful disregard for this policy in my actions may make me liable for action in accordance with the Organisation's disciplinary procedures.

On completion below, I confirm that I will adhere to the content of this statement.

Name	
Title	
Department	
Organisation	
Date of Acceptance	
Signature	
Name of line manager	

Your line manager should retain a signed copy, to be held in your personal file, and an electronic copy should be mailed from your mailbox to:

WHICTS.InformationSecurity@worcsacute.nhs.uk

Appendix 2 - 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 one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	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?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**		
6.	**What alternatives are there to achieving the policy/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact Assistant Manager of Human Resources.

Appendix 3 - Financial Risk Assessment

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	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
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	No
	Other comments:	

If the response to any of the above is yes, please complete a business case which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval