Policy		Worcestershire NHS Healthcare ICT Services Making IT Work

Network Security Policy

Department / Service:	IM&T	
Originator:	Ian McGregor	Deputy Director of ICT
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:
The Network Security Policy applies to all business functions and information contained on the Network, the physical environment and relevant people who support the Network.

Key amendments to this Document:

Date	Amendment	By:
Aug 2013	Policy review, minor amendments. Update into Trust format and change term Trust to Organisation	R King

Contents page:

1. Introduction

This document defines the Network Security Policy for Worcestershire Health ICT Services (WHICTS). The Network Security Policy applies to all business functions and information contained on the Network, the physical environment and relevant people who support the Network.

The Network is a collection of communication equipment such as servers, computers, printers, and modems, which has been connected together by cables. The Network is created to share data, software, and peripherals such as printers, modems, fax machines, Internet connections, CD-ROM and tape drives, hard disks and other data storage equipment.

2. Scope of this document

2.1. Scope

This policy applies to all Networks within WHICTS used for:

- The storage, sharing and transmission of non-clinical data and images
- The storage, sharing and transmission of clinical data and images
- Printing or scanning non-clinical or clinical data or images
- The provision of Internet systems for receiving, sending and storing non-clinical or clinical data or images

2.2. Policy Aim

The aim of this policy is to ensure the security of WHICTS Network. To do this the Organisation will:

- Ensure that the Network is for users
- Protect the Network from unauthorised or accidental modification ensuring the accuracy and completeness of the organisation's assets
- Protect assets against unauthorised disclosure

2.3. Objectives

The objectives of the 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.

- Establishes the security responsibilities for Network security.
- Provides reference to documentation relevant to this policy.

3. Definitions

CCTA	Consumer Credit Trade Association
CD-ROM	Compact Disc Read-only Memory
CRAMM	CCTA Risk Analysis and Management Method
ICT	Information & Communication Technology
IAA	Information Asset Administrator
IAO	Information Asset Owner
IG	Information Governance
IGT	Information Governance Toolkit
ISO	International Organisation for Standardisation
IM&T	Information Management & Technology
IT	Information & Technology
ITSEC	Information Technology Security Evaluation Criteria
NHS	National Health Service
NHSCFS	NHS Counter Fraud Services
PC	Personal Computer
SIC	Statement of Internal Control
SIRI	Serious Incidents Requiring Investigation
SIRO	Senior Information Risk Officer
WHICTS	Worcestershire Health Information & Communication Technology Services

4. Responsibilities and Duties

4.1. Security Responsibilities

- The Chief Executive is the accountable officer for Information Risk Management. The Senior Information Risk Officer (SIRO) is responsible for ensuring the Information Risk Policy is developed, implemented reviewed and its effect actively monitored. The SIRO provides the focus for the assessment and management of information risk at Board level, providing briefings and reports on matters of performance, assurance and cultural impact.
- The Information Asset Owner 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.

4.2. Network Manager’s Responsibilities

- Produce and implement effective security countermeasures.
- Risk asses the network in line with the Organisation’s Risk Assessment Policy.
- Produce all relevant security documentation, security operating procedures and contingency plans reflecting the requirements of the Network Security Policy.
- Ensure all such documentation will be included in the WHICTS asset register.
- Ensure that accurate diagrams of the network architecture are maintained.
- Ensure that all network hardware is included in the WHICTS asset register.

4.3. Information Security Manager's Responsibilities

- Acting as a central point of contact on information security within the organisation, for both staff and external organisations.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Produce organisational standards, procedures and guidance on Information Security matters for approval by Organisations Information Governance Steering Group.
- Co-ordinate information security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on information security matters, including representing the organisation on cross-community committees.
- Working closely with those responsible for Freedom of Information, Data Protection, patient confidentiality and other Information Governance work areas.
- Advising users of information systems, applications and Networks of their responsibilities.
- Ensure breaches of policy and recommended actions are reported in line with Organisation's procedures.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Representing the organisation on internal and external committees that relate to IT security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Providing a central point of contact on IT security issues.
- Providing advice and guidance on:

  i. Policy Compliance
  ii. Incident Investigation
  iii. IT Security Awareness
  iv. IT Security Training
  v. IT Systems Accreditation
  vi. Security of External Service Provision
  vii. Contingency Planning for IT systems

4.4. WHICTS Responsibilities

The WHICTS information Network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information. The Network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, WHICTS will undertake to the following.

WHICTS will:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.
- Provide both effective and cost-effective protection that is commensurate with the risks to its Network assets.
- Implement the Network Security Policy in a consistent, timely and cost effective manner.
- Where relevant, WHICTS will comply with:
  - Copyright, Designs & Patents Act 1988
  - Access to Health Records Act 1990
  - Computer Misuse Act 1990
  - The Data Protection Act 1998
  - The Human Rights Act 1998
  - Electronic Communications Act 2000
  - Regulation of Investigatory Powers Act 2000
  - Freedom of Information Act 2000
  - Health & Social Care Act 2001
- Comply with other laws and legislation as appropriate.
- Ensure the policy must be approved by the Information Security Manager and Data and Communications Manager for WHICTS.
- Ensure that all staff, where appropriate, have access to training in the use of the network.
- Ensure that there are formal request procedures to set up users with network accounts.
- Ensure that any inappropriate use will be identified and reported to the appropriate line manager, IG Lead Manager, Caldicott Guardian and/or Human Resources.
- Where appropriate, disclose evidence of any member of staff contravening the law or professional standards to the police and or/regulatory bodies, including the NHS Counter Fraud Services (NHSCFS).
- Implement and maintain anti-virus software on servers, PCs and laptops

WHICTS will not:

- Routinely monitor individual user's activity.

4.5. Line Manager's Responsibilities

- Ensuring the security of the Network used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Ensuring that their staff are made aware of their security responsibilities.
- Ensuring that their staff have had suitable security training.

4.6. General Responsibilities

All personnel or agents acting for the organisation have a duty to:

- Safeguard hardware, software and information in their care.
- Prevent the introduction of malicious software on the organisation's IT systems.
- Report on any suspected or actual breaches in security.

5. Legislation

The Worcestershire Local Health 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 Local Health Community, who may be held personally accountable for any breaches of network security for which they may be held responsible, failure to comply could result in the individual or the Organisation being prosecuted. The Worcestershire Local Health Community shall comply with the legislation, detailed in section 6, and other legislation as appropriate.

6. Policy Detail

6.1. Document Framework

Document Title	Content	Review period
Network 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 ▪ Information Security ▪ Internet and Email Access ▪ Mobile Devices	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. Risk Assessment

- WHICTS will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the Network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.
- Risk assessment will be conducted to determine the ITSEC Assurance levels required for security barriers that protect the Network.
- Formal risk assessments will be conducted using CRAMM and will conform to ISO17799.

6.3. Physical and Environmental Security

- Network computer equipment will be housed in a controlled and secure environment. Critical or sensitive Network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.
- Critical or sensitive Network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.
- Critical or sensitive Network equipment will be protected from power supply failures.
- Critical or sensitive Network equipment will be protected by intruder alarms and fire suppression systems.
- Smoking, eating and drinking is forbidden in areas housing critical or sensitive Network equipment.
- All visitors to secure Network areas must be authorised by a senior member of the IT department
- All visitors to secure Network areas must be made aware of Network security requirements.
- All visitors to secure Network areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out.
- The Data and Communications Manager will ensure that all relevant staff is made aware of procedures for visitors and that visitors are escorted, when necessary.

6.4. Access Control to Secure Network Areas

- Entry to secure areas housing critical or sensitive Network equipment will be restricted to those whose job requires it. The Data and Communications manager will maintain and periodically review a list of those with unsupervised access.

6.5. Access Control to the Network

- Entry to secure areas housing critical or sensitive Network equipment will be restricted to those whose job requires it. The Data and Communications manager will maintain and periodically review a list of those with unsupervised access.

- Access to the Network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Access will be based on a user's entry on the Active Directory. Remote access to the Network will conform to the Organisation's Remote Access Policy.
- There must be a formal, documented user registration and de-registration procedure for access to the Network.
- Departmental managers must approve user access.
- Access rights to the Network will be allocated on the requirements of the user's job, rather than on a status basis.
- Security privileges (i.e. 'superuser' or Network administrator rights) to the Network will be allocated on the requirements of the user's job, rather than on a status basis.
- All users to the network will have their own individual user identification and password
- Users are responsible for ensuring their password is kept secret
- User's access rights will be removed or reviewed for those users who have left the Trust or changed jobs, in a timely manner.

6.6. Wireless network access

- Access to the network wirelessly will also be in accordance with the requirement of this policy. There will also be additional access controls via certificate and radius servers.

6.7. Third Party Access Control to the Network

- Third party access to the Network will be based on a formal contract that satisfies all necessary NHS security conditions; contractors must complete and receive approval for the Confidentiality Agreement for Contractors and Third Parties
- All third party access to the Network must be logged

6.8. External Network Connections

- Ensure that all connections to external Networks and systems have documented and approved System Level Security Policies.
- Ensure that all connections to external Networks and systems conform to the NHS-wide Network Security Policy, Code of Connection and supporting guidance.
- The Data and Communications Manager must approve all connections to external Networks and systems before they commence operation.

6.9. Maintenance Contracts

The Data and Communications Manager will ensure that maintenance contracts are maintained and periodically reviewed for all Network equipment. All contract details will constitute part of the Asset register

6.10. Data and Software Exchange

Formal agreements for the exchange of data and software between organisations must be established and approved in line with IGT requirements.

6.11. Fault Logging

- The Data and Communications Manager is responsible for ensuring that a log of all faults on the Network is maintained and reviewed. A written procedure to report faults and review countermeasures will be produced.

6.12. Security Operating Procedures (SyOps)

- Produce Security Operating Procedures (SyOps) and security contingency plans that reflect the Network Security Policy.
- Changes to operating procedures must be authorised by the Data and Communications Manager.

6.13. Network Operating Procedures

- Documented operating procedures should be prepared for the operation of the Network, to ensure its correct, secure operation.
- Changes to operating procedures must be authorised by the Data and Communications Manager.

6.14. Data Backup and Restoration

- The Communications Manager is responsible for ensuring that backup copies of Network configuration data are taken regularly.
- Documented procedures for the backup process and storage of backup tapes will be produced and communicated to all relevant staff.
- All backup tapes will be stored securely and a copy will be stored off-site.
- Documented procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
- Users are responsible for ensuring that they backup their own data to the Network server.

6.15. User Responsibilities, Awareness and Training

- The Organisation will ensure that all users of the Network are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.
- All users of the Network must be made aware of the contents and implications of the Network Security Policy and SyOps.
- Irresponsible or improper actions by users may result in disciplinary action(s).

6.16. Accreditation of Network Systems

- Ensure that the Network is approved by the Data and Communications Manager before it commences operation; ensuring that the Network does not pose an unacceptable security risk to the organisation and meets IGT requirements.

6.17. Security Audits

- Information Security will require checks on, or an audit of, actual implementations based on approved security policies and in line with IGT requirements.

6.18. Malicious Software

- Ensure that measures are in place to detect and protect the Network from viruses and other malicious software.

6.19. Secure Disposal or Re-use of Equipment

- Ensure that where equipment is being disposed of, IT Department staff must ensure that all data on the equipment (e.g. on hard disks or tapes) is securely overwritten. Where this is not possible IT Department staff should physically destroy the disk or tape.

- Ensure that where disks are to be removed from the premises for repair, where possible, the data is securely overwritten or the equipment degaussed by the IT Department. Further details are available in the IT Equipment Disposal Policy

6.20. System Change Control

- Ensure that the Data and Communications Manager reviews changes to the security of the Network, in line with Change Control procedures. Responsible for updating all relevant Network Security Policies, design documentation, security operating procedures and Network operating procedures; in line with IGT and Information Security requirements.

- Ensure checks on, or assessment of, the actual implementation based on the proposed changes; in line with IGT and Information Security requirements.

- Ensuring that selected hardware or software meets agreed security standards IGT and Information Security requirements.

- Acceptance testing of all new Network systems will be carried out, in line with IGT and Information Security requirements, in an attempt to cause a security failure and document other criteria against which tests will be undertaken prior to formal acceptance.

- Testing facilities will be used for all new Network systems. Development and operational facilities will be separated.

6.21. Security Monitoring

- Ensure that the Network is monitored for potential security breaches. All monitoring will comply with current legislation.

6.22. Reporting Security Incidents and Weaknesses

- All potential security breaches must be investigated and reported to Information Security; Security incidents and weaknesses must be reported in accordance with the requirements of the Organisation's incident reporting procedure.

6.23. System Configuration Management

- Ensure that there is an effective configuration management system for the Network.

6.24. Business Continuity and Disaster Recovery Plans

- Ensure that business continuity plans and disaster recovery plans are produced for the Network.
- The plans must be reviewed by the Information Asset Owner and tested on a regular basis.

6.25. Unattended Equipment and Clear Screen

- Users must ensure that they protect the Network from unauthorised access. They must log off the Network when finished working.
- The Organisation operates a clear screen policy that means that users must ensure that any equipment logged on to the Network must be protected if they leave it unattended, even for a short time. Workstations must be locked or a screensaver password activated if a workstation is left unattended for a short time.
- Users failing to comply will be subject to disciplinary action.

6.26. Guidelines

- Detailed advice on how to determine and implement an appropriate level of security is available from the Data and Communications 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. 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&13	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

This policy should be reviewed every 2 years under the authority of the Chief Executive. Associated information security standards should be subject to an on-going development and review programme.

10. References:

Access to Health Records Act	1990
Caldicott Principles	
Care Quality Commission	2009
Common Law Duty of Confidentiality	
Computer Misuse Act	1990
Confidentiality: NHS Code of Practice	2006
Copyright, Designs and Patents Act	1988
Criminal Justice and Public Order Act	1994
Data Protection Act/ Processing of Sensitive Personal Data Order	1998/2000
Electronic Communications Act	2000
Freedom of Information Act	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	2005
Records Management: NHS Code of Practice	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, key document is held in control document.

11.2. Financial risk assessment

No business case has been completed as nothing highlighted as a result of the Financial Risk Assessment, key document held in control document.

11.3. Consultation Process

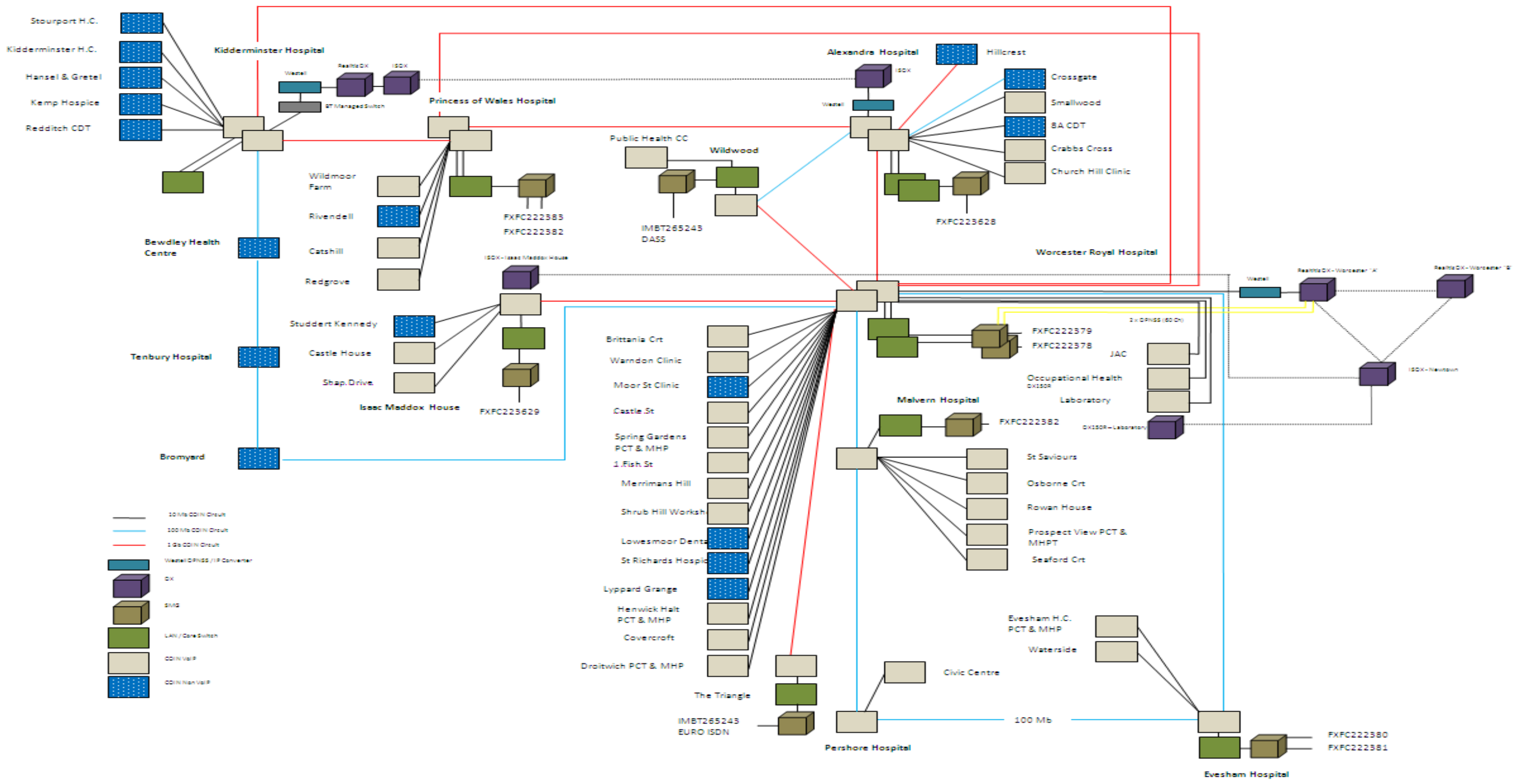
The following stakeholders have been consulted during the production of this Policy:

WHICTS
Information Governance Groups at Organisation and County level

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 held in control document.

Appendix 1


Stourport H.C.
Kidderminster H.C.
Hansel & Gretel
Kemp Hospice
Redditch CDT
Kidderminster Hospital
Westell
RealVis DX
ISDX
BT Managed Switch
Princess of Wales Hospital
Wildmoor Farm
Rivendell
Catshill
Redgrove
FXFC222383
FXFC222382
Bewdley Health Centre
ISDX - Isaac Maddox House
Studdert Kennedy
Castle House
Shap.Drive
Isaac Maddox House
FXFC223629
Tenbury Hospital
Bromyard
Public Health CC
Wildwood
IMBT265243
DASS
Alexandra Hospital
ISDX
Westell
Hillcrest
Crossgate
Smallwood
8A CDT
Crabbs Cross
Church Hill Clinic
FXFC223628
Worcester Royal Hospital
Westell
RealVis DX - Worcester 'A'
RealVis DX - Worcester 'B'
2 x DPNSS (60 Ch)
FXFC222379
FXFC222378
JAC
Occupational Health
DX150R
Laboratory
ISDX - Newtown
DX150R – Laboratory
Brittania Crt
Warndon Clinic
Moor St Clinic
Castle St
Spring Gardens PCT & MHP
1.Fish St
Merrimans Hill
Shrub Hill Worksh
Lowesmoor Denta
St Richards Hospic
Lyppard Grange
Henwick Halt PCT & MHP
Covercroft
Droitwich PCT & MHP
The Triangle
IMBT265243
EURO ISDN
Malvern Hospital
FXFC222382
St Saviours
Osborne Crt
Rowan House
Prospect View PCT & MHPT
Seaford Crt
Evesham H.C. PCT & MHP
Waterside
Civic Centre
100 Mb
Pershore Hospital
FXFC222380
FXFC222381
Evesham Hospital
10 Mb CDIN Circuit
100 Mb CDIN Circuit
1 Gb CDIN Circuit
Westell DPNSS / IP Converter
DX
SMG
LAN / Core Switch
CDIN VoIP
CDIN Non VoIP

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 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.

Supporting Document 2 – Financial Impact 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 and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval