Anti-Virus 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 purpose of this Policy is to mitigate against the threat of damage to Person Identifiable Data (PID), confidential or sensitive information from malicious computer viruses, this is an increasing risk as the number of computer based applications grows.

Key amendments to this Document:

Date	Amendment	By:
Aug 2013	Reformatted into latest Organisation format, minor content updates	R King

Contents page:

1. Introduction

The software and hardware that make up the computer networks are essential resources for NHS Organisations. They aid staff in carrying out their everyday duties and without them important communication systems would not exist.

Computer viruses pose considerable risks to these systems. They can cause them to run erratically, cause loss of information, and information to become corrupted, with the consequential loss of productivity for the Organisation.

2. Scope of this document

2.1 Scope

This policy applies to:

- All employees whilst using Organisation equipment and accessing the Organisation's network at any location, on any computer or Internet connection.
- Other persons working for the Organisation, persons engaged on business or persons using equipment and networks of the Organisation.
- Anyone granted access to the network.

2.2 Policy Aim

Ensure:

- All staff are aware of their responsibilities in relation to safeguarding the confidentiality, integrity, and availability of data and software within the Organisation.
- Best practice concerning the use of software within the Organisation is identified.
- Instructions are provided on the prevention of virus infection, and what steps to take should a virus be found

2.3 Objectives

This policy is designed to give guidance and direction on minimising the risk of a virus infection, and what to do if they are encountered.

Breaches of this policy should be regarded as serious misconduct which could lead to disciplinary action in accordance with the Organisation's Disciplinary Policy.

Every individual defined within the scope of this document is responsible for the implementation of this policy whilst operating any personal computer resources to access any of the organisations systems.

3. Definitions

CD	Compact Disk
HSCIC	Health & Social Care Information Centre
ICT	Information & Communication Technology
IG	Information Governance
IGSG	Information Governance Steering Group
IM&T	Information Management & Technology
IT	Information Technology
NHS	National Health Service
PC	Personal Computer
PID	Person Identifiable Data
SIC	Statement of Internal Control
SIRI	Serious Incident Requiring Investigation
USB	Universal Serial Bus
WHICTS	Worcestershire Health Information & Communication Technology Services

4. Responsibilities and Duties

4.1 WHICTS Responsibilities

WHICTS will ensure that all Organisation PC's and devices connected to the network will have virus-scanning software installed, active and updated regularly.

4.2 User Responsibilities

Users should familiarise themselves and adhere to this policy, in order to minimise the risk by applying good practice to avoid viruses and how to handle them when encountered.

5. Legislation

The Worcestershire Local Health Community is obliged to abide by all relevant UK and European Union legislation.

The HSCIC have also produced the following Good Practice Guideline:

http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/avmal2.pdf

6. Policy Detail

6.1 Document Framework

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

- A virus is a self-replicating piece of software, which may cause damage to the operating system of the computer, the storage devices, and any data and/or software stored on them.
- Software is a computer program that is designed to carry out specific functions.
- A personal computer is any one of the following. Desktop computers, laptop computers, hand held computers.

6.3 Use of Email and Internet

- Email is one of the main ways used to distribute computer viruses. This is due to the ease of which information can be distributed globally. Viruses can be hidden in email attachments or in material downloaded from the internet.

- To help protect against viruses being distributed over the network, the following should be applied:
  - Make sure you know the sender of the email to be genuine before opening any attachments. If you are suspicious in any way then contact the sender by phone, to confirm they have sent the email.
  - If you believe you have received an email virus, or have received an alert from your PC to this effect then please contact the IT Service Desk.
  - Do not download non-business software, screen savers, or any games from any source.
  - Do not action any emails that suggest they have been sent to fix a problem with your machine (e.g. Emails from Microsoft). Reputable vendors would never distribute software patches in this way.

- **If you have any suspicions regarding a received email, do not open it, but contact the IT Helpdesk immediately.**

6.4 Ant-Virus Controls

Requirements:

- Anti-Virus software must only be installed and configured by IT Services. Users must not disable or interfere with anti-virus software installed on any computer.
- No computer may be connected to the network without adequate protection i.e. up to date anti-virus software being installed and activated. Only portable devices owned by the Organisation may be connected to the network, and in line with the Organisation’s policy on connection.
- Portable device users must connect their device to the network every time they change their network password to ensure that their device remains synchronised with their current password and to ensure that the anti-virus software remains updated. Failure to do so could result in unnecessary virus outbreaks and forgotten passwords.
- NHS portable devices must not be connected to non NHS Networks.
- Users must not change or delete any anti-virus software that is installed on the Organisations network.

Software Controls

No software programs or executable files should be downloaded from the Internet and installed onto a PC without the consent of IT Services. Unauthorised downloading of software may breach the copyright licence, could introduce a computer virus to the system, and is a breach of the Organisations Internet Policy.

The unauthorised copying of software is a criminal offence under the Copyright, Design and Patents Act 1998.

6.5 Avoiding Virus Infection

To avoid being infected by a virus:

- Avoid the transfer of information by floppy disk, CD or USB memory sticks between computers and do not introduce the above media from home onto NHS computers.
- Do not “start-up” a PC with a disk in the disk drive, unless instructed by IT Services.
- Make regular backups, store on your local directory and do not store information on the PC so that if infection does occur, data can be recovered.
- All email attachments are checked for viruses as part of the automated process.

6.6 What to do if a virus is found or suspected.

If you find or suspect a virus on your PC:

- Contact the IT Service Desk immediately.
- Do not use the PC until re use has been approved by the IT Helpdesk.

The responsibilities of IT Services are to:

- Check the infected PC
- Check any media that have been used in the infected PC
- Check any other PC that the media has been used with
- Delete or clean any infected files
- Check any Servers that may have been accessed during the incident
- Inform the Information Security Manager of any viruses detected
- Ensure that the incident is addressed within the timescale allocated for the priority.

6.7 Hoax Viruses

Normally received via email (e.g. chain letters), this is an unconfirmed warning or plea with a request that you send the message to everyone you know. If you receive any of this kind of message.

Do not send warnings to other users.
This will then prevent the spread of hoax viruses.

6.8 Information Protection

Staff must wherever possible make use of their home (H) or shared (M) drives for storage of information.

However, where a file server is unavailable, then adequate backups of essential information and software should be taken, so if necessary, any data or software that is lost or corrupted due to virus infection can be recovered quickly under the instruction of IT Services.

6.9 Data Protection

The Data Protection Act governs the processing of personal identifiable data, and protecting the data from loss, damage or destruction, whether accidental or deliberate. This includes having anti-virus controls in place to safeguard information and ensure the Act is complied with.

The security measures must take into account the harm that may result from unauthorised or unlawful processing, loss, damage or destruction. The nature of the data being protected also needs to be considered.

Appropriate personnel checks need to be taken to ensure the integrity of the staff that have access to the data being protected.

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 annually.

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	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	2009
Common Law Duty of Confidentiality	
Computer Misuse Act	1990
Confidentiality: NHS Code of Practice	2003
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.

11.2 Financial Risk Assessment

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

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.

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