Anti Virus Policy

Department / Service:	**IM & T Department**	
Author:	Ian McGregor	Deputy Director of ICT
Status	Draft	**Version** 1.0
Date	23rd September 2008	
Circulation	ICT Programme Board	
Review date	November 2010	

Table of Contents

1 Introduction

1.1 The need for an Anti-Virus Policy

The software and hardware that make up the computer networks are essential resources for the 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.

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.

2. Anti Virus Policy Statement.

2.1 The Organisation's Policy is to ensure that:

- 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

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

2.3 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.

2.4 Scope

This policy applies to:

- All employees whilst using Trust equipment and accessing the Trusts' 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.

2.5 Definitions

- For the scope of this policy, a virus is defined as 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.
- For the scope of this policy, software is defined as a computer program that is designed to carry out specific functions

- For the scope of this policy, a personal computer is defined as any one of the following. Desktop computers, laptop computers, and hand held computers.

3. Use of E-mail and the internet

3.1 E-mail 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.

3.2 To help protect against viruses being distributed over the network, the following should be applied:

- Make sure you know the sender of the e-mail 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 e-mail.
- If you believe you have received an e-mail virus, or have received an alert from your PC to this effect then please contact the IT Helpdesk.
- 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.

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

4. Anti-Virus Controls.

4.1 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 Trust may be connected to the network, and in line with the organisation's policy on connection.
- Portable device users must regularly connect to the network to ensure that the anti-virus software remains updated. Failure to do so could result in unnecessary virus outbreaks.
- 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 Trusts network.

4.2 Software Controls.

4.2.1 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 Trusts Internet Policy.

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

4.3 Avoiding virus infection

4.3.1 To avoid being infected by a virus:

- Avoid the transfer of information by floppy disc, 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 floppy disk in the disk drive, unless instructed by IT Services.
- Where practical write protect floppy disks until the write option is required.
- 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.

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

5.1 If you find or suspect a virus on your PC:

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

5.2 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 Officer of any viruses detected
- Ensure that the incident is addressed within the timescale allocated for the priority.

6 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.

7 Information Protection

Staff must wherever possible make use of their home 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.

8 Data Protection Act 1998

8.1 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.

8.2 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.

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

9. Review and Maintenance

This policy will be subject to annual review and if revised all staff will be alerted to the new version.

This policy has been developed and is monitored by the Information Security Officer.