IM&T POLICY & PROCEDURE
(IM&TPP 01)

Anti-Virus Policy

<table>
<thead>
<tr>
<th>DOCUMENT INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author:</strong> Vince Weldon – Associate Director of IM&amp;T</td>
</tr>
<tr>
<td><strong>Approval:</strong> Executive</td>
</tr>
<tr>
<td><strong>This document replaces:</strong> IM&amp;T Policy No. 1 Anti Virus Version 003.03 July 2012</td>
</tr>
<tr>
<td><strong>Notification of Policy Release:</strong> Distribution by Communication Managers All Recipients e-mail Staff Notice Boards Web-site</td>
</tr>
<tr>
<td><strong>Equality Impact Assessment:</strong> Stage 1 Equality Impact Assessment – No issues</td>
</tr>
<tr>
<td><strong>Date of Issue:</strong> December 2013</td>
</tr>
<tr>
<td><strong>Next Review:</strong> November 2016</td>
</tr>
<tr>
<td><strong>Version:</strong> IM&amp;TPP No. 1 Version 003.04 13 10 14</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1. Purpose

This policy applies to the use of all ICT equipment in use within South Central Ambulance Service NHS Foundation Trust (SCAS). It sets the standards for the deployment of antivirus software, states the position of the Trust and sets out the obligations that all members of staff have in ensuring the security and stability of the corporate infrastructure. This policy is designed to protect the Trust and individuals.

The Trust’s intention 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.

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.

ICT facilities are primarily provided to enable staff to perform their duties and to better conduct the business of the Trust. Only ICT equipment which is the property of the Trust and appropriately protected for such use can be connected to the corporate infrastructure.

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

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

1.2 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 “apps” (an abbreviation for applications) is a piece of software which can run on a personal computer.
• For the scope of this policy, a personal computer is defined as any one of the following. Desktop computers, laptop computers, hand held computers or tablet devices or smart phones.
• For the scope of this policy electronic media is described as any magnetic or electronic device which can be used to record and store data for use on a personal computer.

1.3 Computer viruses

Computer "viruses" are malicious programs which can be unwittingly copied between computer systems. Their effect is to damage, destroy or prevent access to data. The most common way for a virus to infiltrate a system is by the introduction of an "infected" data stick or CD, or infected files downloaded via the Internet or e-Mail. Other devices can become infected through use on an affected system.

Though the Trust deploys software that can assess downloaded files to check that they are virus free it is the responsibility of each individual user to ensure that this is done on files or media that they are accessing or using.

1.4 Virus on networks

Networked systems are particularly susceptible to the spread of viruses once introduced. For this reason SCAS takes Network Security very seriously. The corporate network infrastructure is connected to NHSnet and its own Virtual Private Networking infrastructure via Firewalls, which provide some protection by filtering traffic according to source, destination and type of message.

Strict rules are in place to ensure that all connections via the Firewall are legitimate and authorised by the Associate Director of IM&T or the Head of IT. The rules and connections are reviewed annually by the Trusts IM&T Control Board.

Anti-virus software is installed on all SCAS servers. The actual software will be approved by the Trusts IM&T Control Board following recommendation from the Associate Director of IM&T. The name of the software, or the manufacturer will not be disclosed in writing, or verbally, without the express permission of the Associate Director of IM&T to any third party to better protect network security.

The Associate Director of IM&T or the Head of IT must authorise the connection of any workstation to the corporate Infrastructure.

All devices operating on the network will employ resident virus check and removal programs, these may be resident to the individual device or distributed from within the infrastructure.

It will be considered a disciplinary offence for any member of staff to knowingly bypass this software, or ignore any warning messages that might be given.

2. PRECAUTIONS

2.1 Anti-virus precautions
All computer systems connected to the SCAS infrastructure will have disk-resident virus check programs as approved by the Associate Director of IM&T and the Trusts IM&T Control Board. 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.

All Trust servers must be regularly updated in respect of Anti-Virus and other supplier security patches. Arrangements will be made by IT with relevant departments and system suppliers to ensure that this is achieved, or where a supplier cannot approve the relevant update that other arrangements are put in place to protect the system and the overall infrastructure.

Only equipment that is owned or provided by the Trust can be connected to the Trust network. Connecting any other equipment, including mobile telephones/organisers, data sticks, cameras, iPads, tablets or personal laptops is strictly prohibited.

Data sticks and Diskettes are not routinely approved for use on the Corporate ICT equipment. The Associate Director of IM&T will agree with relevant directors and service leads any exceptions. Where approval is given responsibility for ensuring that they are used safely and securely will reside with the relevant line managers and users themselves.

Only encrypted data sticks sourced from the SCAS IT department will be approved for use.

Any data sticks authorised for use by trust staff will require that the data transferred to them is encrypted. The trust will deploy as a minimum standard NHS approved encryption protocols.

Individuals provided with such data sticks will be responsible for routinely checking them prior to use to ensure that they do not contain viruses or other unwanted attachments.

New software applications must only be installed by staff or suppliers approved by the Associate Director of IM&T or the Head of IT. All such applications will be checked to ensure that they are virus free, and that they are legitimately licenced for use on SCAS equipment. Any instances of unlicensed software will be disabled without consultation, and further access will not be permitted without the express authorisation of the Associate Director of IM&T.

No software programs, applications or executable files should be downloaded from the Internet and installed onto a PC without the specific consent of the Associate Director of IM&T or the Head of IT. 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.

Advice on virus scanning and anti-virus software can be obtained from IT support.

2.2 Failure to take precautions

It should be noted that it is a criminal offence under the Computer Misuse Act 1990 to deliberately introduce a virus to a computer system. It shall be a disciplinary offence to introduce a virus to any SCAS computer systems by failing to observe the precautions noted above.

3. VIRUS CONTROL
3.1 Checking for a virus

Master copies media containing important data or program files should be written protected where possible. All line managers are responsible in ensuring that proper precautions as detailed above in para 2.1 are taken when staff are using data sticks, external diskette or downloaded files. When a data stick is issued it will be virus free, it should be recorded appropriately. The record should stipulate the following information:-

- Data stick identifier
- Date anti-virus check was made
- Version number of the anti-virus software used
- Signature and initials of the person carrying out the check

It is the responsibility of the individual user to ensure that the Data stick is rechecked at any time after they have been used on a non-SCAS device.

3.2 When a virus is found

Where a disk, data stick or computer is found to be infected with a virus, the following will apply:-

3.2.1 The ICT Helpdesk will be informed immediately that a virus has been discovered. IT support will then either arrange to attend and deal with the virus OR will confirm with the individual concerned procedures to quarantine or clean the infected disk or computer using the provided Anti-Virus software.

3.2.2 If a data stick or disk is successfully cleaned, a label shall be affixed clarifying that the device has been scanned and is now clean. Where it is not possible to clean the infected device, it shall be clearly marked “VIRUS INFECTED” and given to the relevant Divisional ICT team who will contact the manufacturers of the anti-virus software for further advice in an attempt to isolate and remove the virus. If the IT Department cannot safely eradicate the virus, the disk or data stick will be physically destroyed. There will be no exceptions to this procedure.

3.2.3 The Department Head will be informed in writing that a virus has being detected and measures will be taken to virus test computers and electronic media within that department. Where a computer is suspected to be infected, the computer should be disconnected from the network if attached. The ICT Department keep a log of all computer systems and electronic media checked, also a log will be kept of all virus detected within the SCAS, and action taken to eradicate infections and educate the user.

3.3 Previous Backups

Where a virus is introduced on to a main server within the SCAS infrastructure, the infected server will be immediately disconnected from the network. The infected server will be cleaned and checked to ensure that previous backups taken are not affected before the system is brought back into active use, utilising the most recent “clean” back up available.

3.4 Working Remotely
Staff working away from Trust office locations must ensure that they use the anti-virus facilities resident to their laptops to ensure that any approved data sticks or diskettes are checked prior to being loaded, as well as checking any items downloaded from the Internet.

In the event that they do detect a virus then the infected product must be removed from the Trust equipment and nothing should be downloaded from the disk or data stick. The ICT Service desk should be contacted at the earliest opportunity and arrangements made to have the media and/or laptop inspected by ICT staff to ensure that no infection has taken place before the portable computer is re-connected to the SCAS internal network or electronic media are loaded on to SCAS's computers.
4 REVIEW OF THIS POLICY

This policy will be reviewed 3 years from its date of approval. Reviews may be conducted outside of these times in response to exceptional circumstances or relevant changes in legislation.

5 EQUALITY STATEMENT

The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marital status, disability, race, nationality, gender, religion, sexual orientation, gender reassignment, ethnic or national origin, beliefs, domestic circumstances, social and employment status, political affiliation or trade union membership, HIV status or any other basis not justified by law or relevant to the requirements of the post.

By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of race, ethnic or national origin, colour or nationality; gender (including marital status); age; disability; sexual orientation; religion or belief; length of service, whether full or part-time or employed under a permanent or a fixed-term contract or any other irrelevant factor.

Where there are barriers to understanding e.g an employee has difficulty in reading or writing or where English is not their first language additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resource Department.

6 POLICY MONITORING

The IM&T Directorate of the Trust will be responsible for the monitoring of this policy and its supporting processes and documentation.

Regular reports will be provided to the corporate IM&T Control Board in respect of Virus notifications and remedial action taken.

Where a virus outbreak is reported then the Trust’s Audit and Governance committee’s will be notified as appropriate, including details of findings and remedial action taken.