Western Health and Social Care Trust

MALICIOUS SOFTWARE POLICY

June 2019

Version 2.3

Policy Title	MALICIOUS SOFTWARE POLICY
Policy Reference Number	CORP09/008
Original Implementation Date	September 2009
Revised Dates	November 2014 November 2016 June 2019
Approved Date	ICT SMT Approval – 28/03/2019 Finance SMT Approval – 01/04/2019 Trust CMT – 11/04/2019 Staff Side Consultation – 01/05/2019 Trust Board Approval – 13/06/2019
Review Date	2 years after Trust Approval
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Revised Policy Changes			
Additions:		**Title**	**Comments**
	Section 2, Page 4	Cybersecurity	Inclusion of section specifically related to Cybersecurity. This section will be included in all ICT policies
	Section 6, Page 7	Additional resources	Inclusion of GDPR, FOI, Disposals, ICO, and Data Protection 2018 and other references
	Section 7.1, Page 7	General ICT Training	Now set out on its own
	Section 7.2, Page 7	E-Learning	Includes sub-section for Cyber Security training. This section is being included in all ICT policies
	Appendices	Apendix 1	Remote Access Form
Amendments:			
	Section 1, Page 4	Background and Purpose	Change of term computer to device and providing examples. Expansion of the who constitutes WHSCT Staff
	Section 3, Page 5	Guidelines for Staff	Change word from computer to device Acessing HSC and Non HSC network
	Section 5, Page 6	On Discovery of a Virus or Malware	Expansion of title and change of word computer to Device

Table of Contents

1. Background and Purpose

For the purposes of this document the term device refers to and covers all Trust owned ICT equipment (such as PC's, tablets, smart phones , mobile devices etc)

Malicious software are programs that may cause harm to a device's system's data, performance or networking capabilities. These are commonly known as viruses, Malware or Trojans and they can infect a device without the permission or knowledge of the owner.

The primary sources for malicious software are e-mail attachments, downloads from the Internet and removable media such as memory devices (e.g. USB sticks, Pen drives, Memory cards etc), and CD/DVDs.

The use of the above-mentioned sources can lead to widespread virus infection and damage to systems and data. It is for this reason that the use of these types of removable storage media needs to be strictly controlled.

The purpose of this policy is to minimise the risk of the Trust's network and systems becoming infected with malicious software by making staff aware of the organisation's definition on acceptable and unacceptable use.

The measures outlined in this policy will not be effective without the cooperation of all WHSCT staff. These include full-time, part-time, 3rd party consultants contracted by the Trust to work on specific projects, agency and temporary employees including students and volunteers. The cooperation of all such staff, and acceptance of this policy, is therefore a prerequisite to approval for ICT device use.

2. Cybersecurity

Trust staff need to be aware of the risks and potential for loss of data, equipment or embezzlement of funds via Cyberattacks.

*A **cyberattack** is any type of offensive manoeuvre employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys systems or attempts to embezzle users/businesses.*

Cyberattacks can take multiple forms and the following are a few examples;

- Hacking – someone gaining unlawful access to the ICT network, computer, laptop etc and potentially deleting files and/or stealing data.
- Malware – malicious software that can do any number of things e.g. delete files, make systems crash or target communications equipment.
- Ransomware – where a piece of malicious software runs on a PC, laptop or server, and encrypts (garbles) all the data on the device and therefore makes it no longer usable. There is no guarantee that if the guarantee is paid that the device will decrypt or that encryption will reoccur!
  "Wannacry" was an example of a worldwide ransomware (cyber) attack in May 2017

3. Guidelines for Staff

a) Do **not** install any software onto ICT devices. Only ICT staff have the authority to install software.
b) There is **no issue** with attaching Trust ICT devices (e.g. PC, laptop etc) to HSC networks.
c) If access is required from a Non-HSC network (e.g. from home, hotel etc) then a Remote Access Form needs to be completed, approved (by at least Assistant Director level) and submitted to ICT Service Desk. Upon ICT approval remote software needs to be installed on the device and an authentication device issued.
d) Use of Trust ICT devices is limited to members of Trust staff and for Trust business.

4. Countermeasures

This policy should be seen as one of a number of countermeasures put in place to protect the organisation and its employees from such things as inadvertent exposure to illicit material, malicious software etc, and also the possibility of legal action as a direct result of computer abuse or misuse. The following infrastructure provides primary protection: -

- **Endpoint Security**
  All computers have Endpoint (*anti-Virus)* software installed. The software runs continuously and is updated with the latest version several times a day. Security patches are applied, on a regular basis, to all PC's, servers and laptops that are connected to the Trust network.
  Users of other third party devices/modalities that are attached to the Trust network must make special arrangements to have Endpoint software installed via the ICT Service Desk.
  As part of the Endpoint control measures, certain e-mail attachments are blocked from entering or exiting the HSC network. If an attachment is blocked the user is informed via e-mail of the steps to take to request its release.

- **Firewall**
  A Firewall, utilised regionally by the BSO, provides protection against unsolicited access to the Trust and wider HSC networks. Any unauthorised access or attempts to circumvent these measures will be thoroughly investigated and may result in disciplinary action.

- **Content Filtering**
  All e-mail content (including attachments) is filtered. This technology is used to identify and remove malicious software as well as **blocking** certain e-mail attachments from entering or exiting the HSC network. These include executable file types, music and others.

- **Encryption**
  The Trust allows the receipt and transmission of encrypted e-mails from/to external organisations. Appropriate encryption must be used as approved by the BSO ITS. For more information on how to encrypt e-mails please refer to the procedure listed on the Intranet Website (under ICT, E-mail encryption).

- **Software Updates**
  Some software may contain security vulnerabilities that were not identified prior to its release. These issues can cause programs to run less effectively or make them susceptible to certain malicious software attacks. Depending on the seriousness of the vulnerability, the Trust will distribute updates, known as patches, to all computers connected on the Trust network. Patches will be installed on Trust computers automatically and may require them to restart.

5. On Discovery of a Virus or Malware

a) Contact the ICT Service Desk immediately with as much detail as possible
b) Switch off the device until further notice.

6. Additional Resources

This policy should be read in conjunction with other policies relating to effective and appropriate use of ICT services, including:

1) WHSCT E-mail Policy
2) WHSCT Internet Policy
3) WHSCT Management of User Accounts and Password Policy.
4) WHSCT Server, Desktop and Portable Security Policy
5) WHSCT Protocol for the Electronic Transmission of Confidential Information by Fax and Email
6) WHSCT Social Media Policy
7) WHSCT Disposals Policy (incl redistribution of ICT equipment)
8) WHSCT Data Protection and Confidentiality Policy
9) DOH – Code of Practice on Protecting the Confidentiality of Service User Information
10) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
11) Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
12) Regulation of Investigatory Powers Act 2000
13) Computer Misuse Act 1990
14) General Data Protection Regulation (GDPR)
15) Data Protection Act 2018
16) Freedom of Information (FOI) Act 2000
17) BSO ICT policies

7. Training

The Trust is committed to staff development and seeks to consistently improve development standards and opportunities for staff in line with organisational objectives, policies and procedures.

7.1 General ICT Training

Should you or your staff require support in the effective use of ICT please contact the ICT Training Team via the ICT Service Desk.

7.2 E-Learning - Cyber Security (as defined in Section 2 of this document)

The Western Health and Social Care Trust have invested in a software solution from Metacompliance Ltd to help ensure that the WHSCT ICT security expectations are understood by Trust staff. This is an E-Learning platform which enables the Trust to push out awareness content to Trust staff. This provides education regarding Cyber Security topics and the importance of Good Practice and Trust policies and thereby protects the organisation from potential attack.

This tool is designed to be intuitive and flexible so that Trust staff can easily register and undertake training at a time and place that suits them.

Note: Lessons learnt from this training, e.g. Phishing emails, can also be applied to the individual's home environment.

8. Equality & Human Right's Statement

The Western Health & Social Care Trust's Equality and Human Right's statutory obligations have been considered during the development of this policy.

9. Further Information

For further information in relation to this policy please refer to:-

The ICT service desk portal which is available on the Trust intranet link below.

(http://wta-eservicedesk/portal/)

Appendices

Western Health and Social Care Trust

Appendix 1

Request for a New or Replacement Crypto Card (Remote Access)

Requesting Staff (Please complete in CAPITALS)

Name		Contact No	
Job Title			
Department/Ward		Cost Centre	

Employee Details (Please complete in CAPITALS)

Existing Staff	☐	New Staff	☐	Proposed Start Date	
Name				Staff No.(if known)	
Job Title					
Department/Ward				Contact No	
Location					

Please state Business/ Clinical requirement for **NEW** Crypto Card.

Please state reason for **REPLACEMENT** Crypto Card.

Lost	☐	Stolen	☐	Damaged (Please return damaged device to ICT Dept)	☐

Further Information (Please give brief details of loss or theft.)

Authorisation

Authorised by (Please Print)			
Job Title		Contact no.	
Signature		Date	

ICT Department Use Only

Service Desk Ref No		Account Details	
Date Received		Date Completed	

Completed forms should be returned to ICT Department,
ICT Services Building, Altnagelvin Area Hospital
Glenshane Road, L'Derry, BT47 6SB