Western Health and Social Care Trust

SERVER, DESKTOP AND PORTABLE SECURITY

June 2019

Version 3.2

Western Health and Social Care Trust

Policy Title	SERVER, DESKTOP AND PORTABLE SECURITY POLICY
Policy Reference Number	CORP09/005
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**
	Section1, Page 5	Background and Purpose	Definition of the word Device
	Section 2, Page 5	Cybersecurity	Inclusion of section specifically related to Cybersecurity. This section will be included in all ICT policies
	Section 3, Page 6	ICT Devices and systems	Reminder to staff about GDPR and FOI. Reference to redistributing of devices. Change to HSC and Non HSC network connections Change to wording regarding shared printing
	Section 4, Page 7	Usage	New Section
	Section 7, Page 9	Incident Reporting	New Section
	Section 8, Page 9	Countermeasures	Inclusion of Content Filtering, Encryption
	Section 9, Page 10	Additional Resources	Removal of the word Microsoft Inclusion of GDPR, FOI, Disposals, ICO, and Data Protection 2018 and other references
	Section 10.1, Page 10	General ICT Training	Now set out on its own
	Section 10.2, Page 11	E-Learning	Includes sub-section for Cyber Security training. This section is being included in all ICT policies
	Appendices, Page 12	Apendix 1	User Access Request Form
Amendments:			
	Section 1, Page 5	Background and Purpose	Expansion of the who constitutes WHSCT Staff
	Section 3.1, Page 6	ICT Devices and Systems	Add including redistributuion of ICT equipment reference to end of Disposals Policy comment
	Section 3.2, Page 7	Removable Media	Include Smart Phones
	Section 7, Page 9	Incident Reporting	Ammend to include contacting

			ICT support desk
	Section 8, Page 9	Endpoint Security	Refer to software patches and blocking emails
	Section 8, Page 10	Monitoring	Change of workding regarding breaches in policy

Table of Contents

1. Background and Purpose

The Western Health and Social Care Trust (WHSCT) invests heavily in ICT infrastructure to improve performance and service capability for excellent patient / client care. This investment is supported by increased spending on ICT Governance and information security.

Staff must be aware of the need to secure ICT devices against theft or damage. The information on these devices can be of a highly sensitive nature and need to be protected against unauthorised access.

For the purposes of this policy, the term "device" refers to PC's, Servers, laptops, tablets, smart phones etc, or any "device" used to record/store personal or client data.

All staff have a responsibility in relation to the physical and information security of all the ICT devices and systems they use or have access to.

The policy sets out measures to be adhered to by staff as part of their responsibilities for safeguarding Trust systems and services- and the data they hold – from misuse, abuse, corruption or loss.

The policy also includes guidance for ICT Services staff who have an additional responsibility for ICT equipment and network sustainability.

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

3.1. ICT devices and systems

a) **Only** authorised devices that are owned by the Trust can be used to store or process Health and Social Care information.

b) **Only** authorised devices that are owned by the Trust/HSC can have access to the Trust network.

c) **No** ICT device is to be removed from Trust property without authorised permission. The ICT Service Desk must be informed and appropriate documentation completed. Only authorised members of Trust staff can use ICT devices whether on/off-site

d) All PC's, tablets and laptops **must** have encryption software installed and activated.

e) Staff are reminded that any data recorded on ICT devices and systems, including images and audio, are subject to General Data Protection Regulation (GDPR) and Freedom of Information (FOI) Act 2000

f) Staff carrying or using ICT devices on or off Trust's premises **must** take all reasonable steps to guard against their theft, loss or damage and against unauthorised use.

g) There is **no issue** with attaching Trust ICT devices (e.g. PC, laptop etc) to HSC networks.

h) 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 Deirector level) and submitted to ICT Service Desk. Upon ICT approval remote software needs to be installed on the device and an authentication device issued.

i) Installation (by ICT staff) of new software or hardware, or changes to configurations, is only **permitted** provided appropriate licensing arrangements are in place.

j) The Trust has provided backup arrangements. Users **are advised to** ensure their business data is backed up in order to safeguard against possible data loss. For further details contact the ICT support desk .

k) Only ICT staff are authorised to move ICT devices. Staff should ensure that all requisite documentation (IT Asset Movement Form – refer to Appendix)) must be completed in line with internal ICT procedures.

l) Authorisation must be sought before a 3rd party removes an ICT device from the premises for repair, staff **must** ensure that any sensitive data is protected. Requisite documentation (IT Asset Movement Form – refer to Appendix) must be completed in line with internal ICT procedures.

m) Trust ICT devices should **only** be used for Trust business.

n) Use of unauthorised Cloud services is **prohibited**

o) Any **device** that requires connection to the Trust network must be authorised by the ICT department.

p) With regard to shared printing; staff are **responsible** that information is sent to the correct printer and particular care should be taken in Shared working spaces. Personal identifiable information (letters, reports, etc.) sent to a shared printer should be collected as soon as possible and checked to ensure it is not mixed up with information printed separately or by other staff. This is particularly important to avoid identifiable information being attached and inappropriately sent to the wrong person.

The reader is refered to ICT FAQ's>Printer Management section on **Staff West** (Trust Intranet) for "Instructions for Confidential Printing".

(Note:- All Trust multifunctional printers should have a pin & print capabilities and users should be advised to use these when sharing MFP's)

q) Arrangements **must** be made with ICT staff for the physical disposal of ICT equipment. For further details refer to WHSCT ICT Disposals policy (including redistribution of ICT equipment).

Note: Redistribution of "devices" , containing personal data, is subject to the GDPR and Computer Misuse acts.

3.2. Removable Media

This includes the use of CD ROMs, DVDs, Floppy disks, USB devices (e.g. Memory sticks, Pen drives, Flash drives, External hard drives, Memory cards, Smart phones and any other removable device capable of storing information. This is not an exhaustive list)

a) **NO** identifiable patient/client or business sensitive information should be written onto this type of device, unless-

   i) There is a genuine **business imperative** for doing so
   ii) **AND** approval has been granted under the Data Access Agreement (DAA)
   iii) **AND** the media is fully encrypted and complies with all relevant Communications and Electronic Group (CESG) Standards

b) Patient/client identifiable information currently held on devices that does not meet these standards should be removed immediately. For advice on safe removal of this type please contact ICT Service Desk.

4. Usage

a) Staff must **not** install any software/applications/programs, e.g. Google Chrome.. This function can only be carried out by ICT staff. For advice, users are asked to log a request with the ICT Service Desk

b) In order to ensure that the *latest* Security Patches (e.g. from Microsoft, Sophos etc) are applied; users are **required** to restart their device when notified by "on screen" reminders.
Failure to do so may pose a risk to the Trust and Regional ICT systems by enabling such programs as malware to infect systems and networks.

c) Any data, texts, audio or images recorded by ICT devices are subject to General Data Protection Regulation (GDPR) and Freedom of Information (FOI) Act 2000

d) BSO and the Trust AD for ICT and Telecommunications have the authority to **restrict** access to websites, if any web site is deemed to pose a Cyber security threat or is not in the interests of the Trust.

4.1 Network Accounts and User Profile Storage

Each user will be provided with a storage area, within their user profile, for documents and files e.g. "My documents" folder. User's **should be mindful** that storage space is a limited resource and therefore the ICT department has applied storage restrictions. Users who require an extension to their storage restriction should log a request with the ICT Service Desk.

a) It is the user's **responsibility** to ensure patient/client data is stored appropriately i.e. information relating to patient care should reside within the appropriate system or within the patient medical records

b) Patient and work related Multimedia files (video, photographs, audio, ebooks etc) should **not** be stored in user profiles. For example work related training videos could be stored in "shared areas". In order to discuss a suitable arrangement users are advised to log a request with the ICT Service Desk.

c) **Non Work** related Multimedia files (e.g. personal wedding videos, family photographs etc) should not be saved to Trust Devices. Any such existing files should be **removed**. ICT have the authority to delete any media files that are in breach of any copyright laws (e.g. commercial films and music)

d) Only files and documents relevant to Trust business should be stored within a user profile. Users are **reminded** that all files and documents are discoverable, eg. FOI, GDPR, and should not store personal data on Trust devices.

5. Computer suites and Communication Rooms

a) Controlled access to secure areas is in place. Certain staff roles may necessitate permission to enter these facilities. All requests should be made through the ICT Services Desk for consideration.
b) Where reasonably possible records should be maintained, identifying staff allowed to enter secure areas. Access rights will be reviewed on a regular basis.
c) Access **must** be secured by swipe access or locks, preferably with codes which can be changed periodically.
d) All doors and windows **must** be locked when such rooms are unattended.
e) Supervised visitor access will be authorised for specific purposes at the discretion of the ICT Services. Such visits will be recorded.

f) Eating and drinking in secure areas is prohibited.
g) Computer suites and communications rooms, although secure, should never be used as storerooms.

6. ICT Equipment and Network Security

The creation of a new ICT network domain, including those by 3rd party providers, requires approval from the ICT Department.

7. Incident Reporting

Staff should report any actual or suspected breaches of confidentiality or data security with regard to devices via the Trust's incident reporting procedure.

Staff should report any loss or theft of a Trust owned device, including mobile phones, by ;

i. Reporting any loss to the ICT Support Desk and
ii. By logging a DATIX incident. (Trust's incident reporting procedure)

8. Countermeasures

This policy should be seen as one of a number of countermeasures put in place to protect the organisation and its employees from inappropriate access to systems. Additional protection is provided by the following:-

- **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.

- **Encryption**
  The Trust allows the receipt and transmission of encrypted e-mails from/to external organisations. Appropriate encryption mechanisms 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).

- **Content Filtering**
  All e-mail content (including attachments) is filtered. Content filtering is used to aid the detection and removal of spam e-mail. Filters are refined on a daily basis;

however users may still find these types of messages in their Inbox. Upon discovery users should forward these items to **spam@westerntrust.hscni.net**

- **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.

- **Monitoring**
  i) The Trust reserves the right to perform adhoc inspections, either physically or remotely, to ensure compliance of this policy.
  ii) *Suspected cases of abuse or breaches in policy will be rigorously investigated* by ICT, and where necessary, in conjunction with HR staff.

9. Additional Resources

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

1) WHSCT Email Policy
2) WHSCT Internet Policy
3) WHSCT Management of User Accounts and Password Policy.
4) WHSCT Malicious Software Policy
5) WHSCT ICT Disposals Policy (including redistribution of ICT equipment)
6) WHSCT Social Media Policy
7) WHSCT Incident Reporting Policy and Procedures
8) DOH – Code of Practice on Protecting the Confidentiality of Service User Information
9) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
10) Information Commissioner – Data sharing code of practice (www.ico.gov.uk)
11) Regulation of Investigatory Powers Act 2000
12) Computer Misuse Act 1990
13) General Data Protection Regulation (GDPR)
14) Data Protection Act 2018
15) Freedom of Information (FOI) Act 2000
16) BSO ICT policies

10. 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.

10.1 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.

10.2 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.

11. 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. There are no changes to impact for service users/staff in this updated policy.

12. Further Information

For further information in relation to this policy please contact the ICT Operation Manager.

.

Appendices

Office Moves – IT MOVEMENT REQUEST FORM.

Western Health and Social Care Trust

Please note **4 weeks' notice** is required –
Please log a REQUEST on the Helpdesk and
Keep it up-to-date with changes.

IMPORTANT

The WHSCT Asset Register contains all the information about our ICT Asset information and must be kept up-to-date.

Managers have the responsibility for ALL ICT assets in their Department and must obtain ICT Authorisation before a move.

Requester Name:		Move Date:		Location From		Location To:	

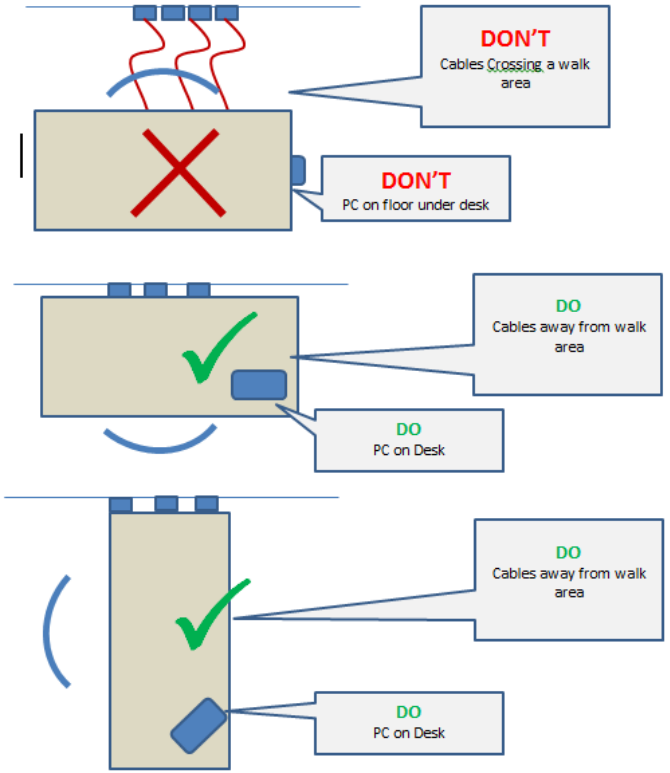
Line Mgr. Signature		Asset No	From Room	To Room	Comments(e.g. Users' Names)

Office Moves – To make the move easier.

1) Each PC / Laptop, Printer, and Phone to have an A4 sheet with the name of its User.

2) Each Desk to have an A4 sheet with the name of its User.

3) Desks must be positioned to avoid power & data cables lying over walk areas. (See below)



*******PLEASE NOTE: Porters and Transport may need to be arranged separately *******