Western Health and Social Care Trust

ICT DISPOSALS POLICY
(Including redistribution of ICT equipment)

June 2019

Version 2.3

Revised Policy Title	**ICT DISPOSALS POLICY** **(Including redistribution of ICT equipment)**
Original Policy Title	*ICT DISPOSALS POLICY*
Policy Reference Number	CORP11/006
Original Implementation Date	November 2011
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 year after Trust Approval
Responsible Officer	FERGAL DUREY, AD for ICT and Telecommunications

Revised Policy Changes			
Additions:		**Title**	**Comments**
	Section 4, Page 5	Cybersecurity	Inclusion of section specifically related to Cybersecurity. This section will be included in all ICT Policies
	Section 6, Page 6	Disposal / Redistribution Procedure	Insertion of line to remind users about GDPR, FOI responsibilities
	Section 6, Page 6	Disposal	Item 2 Refers specifically to the disposal of mobile phones
	Section 8, Page 8	Additional Resources	Inclusion of GDPR and Data Protection 2018 references
	Section 9.1, Page 8	General ICT Training	Now set out on its own
	Section 9.2, Page 8	E-Learning	Includes sub-sections for Mandatory and Cyber Security training. This section is being included in all ICT Policies
Amendments:			
	Section 6, Page 9	Redistribution	Item 1 Enhanced by including working from the Mobile Device Policy regarding Mobile Phones
	Section 8, Page 8	Additional Resources	Updated

Western Health and Social Care Trust

Table of Contents

1. Introduction

This policy should be read in conjunction with any other Western Health and Social Care Trust (WHSCT) policies or guidelines relating to the Disposal of Equipment.

2. Scope

This policy applies to all Western Trust employees and covers all Trust owned ICT equipment.

3. Purpose

The purpose of this document is to set out the process that must be followed for the disposal / redistribution of all ICT related equipment. This includes, but not exclusive to, Personal Computers (desktop, notebook or tablets), Personal Data Assistants (PDAs), printers (including multi-functional devices), scanners, mobile phones, miscellaneous peripheral equipment including network and telecommunications equipment (routers, hubs, switches etc.).

4. 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

5. Applicability

ICT equipment is disposed of under the terms of the Trust's Financial Regulations.

Disposal of ICT equipment may arise as follows:

- The Western Trust ICT Department deems the ICT equipment has reached it's "'end of life" in accordance with current replacement guidelines.
- The ICT Department has deemed that the ICT equipment is un-repairable or has reached a stage where it is considered to be Beyond Economic Repair (BER)

Redistribution of ICT equipment may arise in the following circumstances. This list is not exhaustive:

- When a person is leaving their post
- Where a piece of ICT equipment is reassigned to a different employee and/or office within a department/facility/site.
- As part of any ICT equipment upgrade the equipment is removed and returned to the ICT department.

6. Disposal / Redistribution Procedure

- When a piece of ICT equipment is no longer required **OR** is to be reassigned, a member of Trust staff should contact the ICT Service Desk and log a work request. This request will be assigned to the ICT Operations Manager

  Users are reminded of their responsibilities regarding GDPR, FOI etc.

- The ICT Operations Manager will decide on the appropriate course of action and update the ICT Asset Register, including any software records or licensing paperwork, to reflect a change.

- Disposal
  1. Storage media will be physically removed from any ICT equipment and after a period, of 3 months, will be given to a licensed 3rd party contractor for safe disposal. This contractor will provide certificates verifying that storage media has been safely disposed. The certificates will include the asset numbers of the originating hardware and the serial numbers of the storage media. (Where storage media cannot be removed, the device will be made inactive or disposed of by Trust ICT staff in line with WEEE directive) The remaining components will be disposed of in line with WEEE guidelines.
  2. Trust mobile phones - it is ***the user's responsibility*** to transfer any contact details to another device before surrendering for disposal. Trust Mobile phone SIMS and memory cards will be physically destroyed and will not be recoverable. The ICT department is not liable for the retrieval of data recorded on any mobile phone, SIM and memory cards.

- Redistribution
  1. Should an employee, or manager, have cause to transfer a Trust computer, laptop, mobile phone or device to another member of staff within the Directorate/Department they should log the details of the transfer on the ICT Helpdesk.

     Redistribution of "smart" phones, containing personal data, is subject to the GDPR and Computer Misuse acts.

     The following details should be provided to the Helpdesk;

- Mobile number
- Current user
- New user
- Department
- Directorate
- Cost centre

2. Managers are advised to consult with the ICT Operations Manager if they have any doubts or queries regarding the redistribution of ICT equipment.
3. Any ICT equipment which has been returned to the ICT department may be redistributed by the ICT Operations Manager depending on the needs of the service. Any ICT equipment, containing internal storage, being redistributed will be reimaged beforehand.
4. Redistribution of ICT equipment is the sole responsibility of the ICT department.

- The AD for ICT and Telecommunications will regularly review and authorise an ICT disposal list. This list will, in turn, be presented to a nominated officer, at AD level, in Finance for disposal authorisation.
- ICT hardware (where storage media has been removed), will be disposed of by external waste contractors who comply with all environmental regulations including WEEE directive. The contractors will provide certificates verifying disposal in accordance with WEEE directive. The certificates will include the asset numbers, where possible, and serial numbers for disposed equipment.
- ICT Asset Register will be updated to reflect that equipment is now *disposed / redistributed.*

7. Guidelines for staff

Any Personal Computer, or media storage device (e.g. external disk, USB memory sticks), which are supported by the Western Trust is considered as an information governance risk and has the potential for unlawful disclosure under the Data Protection Act 2018 and must be disposed of in the correct manner by ICT.

Line managers should ensure that ***all*** PCs, laptops and tablets in their department are backed up on a regular basis. Backup utilities are available on all PC's and if assistance is required, staff should contact the ICT Support Desk.

An "ICT Equipment Movement Form" must be completed and returned, for approval, to the ICT Operations Manager prior to any ICT equipment redistribution.

Before any device is transferred to ICT services for disposal / redistribution, the departmental line manager should ensure that all stored data is backed up so as to ensure Business Continuity. This will thereby fulfil the Trust FOI requirements. Once removed for disposal / redistribution ICT *cannot* guarantee recovery of the data!

Line managers need to ensure that appropriate arrangements are made to enable accessibility in line with departmental business processes.

***ALL* Trust owned ICT equipment *must be* submitted to ICT services for safe disposal.**

Disposal / redistribution of ICT equipment by any other means may leave the Trust liable in the event of a fault or loss of data.

8. Additional Resources

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

1) WHSCT - Internet Policy
2) WHSCT - Management of User Accounts and Password Policy.
3) WHSCT - Server, Desktop and Portable Security Policy
4) WHSCT - Malicious Software Policy
5) WHSCT Data Protection & Confidentiality Policy
6) WHSCT - Social Media Policy
7) *Freedom Of Information & E-mails Guidance (issued by WHSCT Communications Department)*
8) Information Commissioner – Anonymisation: managing data protection risk – code of practice (www.ico.gov.uk)
9) Any disposal of equipment policy or guidelines produced by Estates Services or Financial Services.
10) General Data Protection Regulation (GDPR)
11) Data Protection Act 2018
12) WHSCT - Waste Manual:- Section 5.1 Waste Electrical and Electronic Equipment (WEEE)
13) BSO ICT policies

9. 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.

9.1 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.

9.2 E-Learning - Cyber Security **(as defined in Section 4 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.

10. 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.

11. Further Information

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