Belmont House, 57 Belmont Road, Cambuslang, G72 8PG
www.wwhc.org.uk E: enquiries@wwhc.org.uk T: 0141 641 8628

Policy Name	**Disposal of IT Equipment**
Policy Author	**Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**August 2022**
Latest date of Next Review	**September 2027**

West Whitlawburn Housing Co-operative will provide this policy on request at no cost, in larger print, in Braille, in audio or other non-written format, and in a variety of languages. Please contact the office.

HAPPY TO TRANSLATE

Registered with the Scottish Housing Regulator No. 203
Registered Charity No. SCO38737, VAT Registration No. 180223636
Registered society under the Co-operative and Community Benefit Societies Act 2014

1. Introduction

1.1. This policy gives guidance on the appropriate destruction of IT equipment and other media. The policy is part of WWHC's Information Security Management System and takes into account freedom of information, data protection, and environmental protection legislation.

1.2. This policy aims to ensure:

- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.
- Compliance with Data Protection Act 2018 through secure disposal or preservation of personal data.
- Compliance with Freedom of Information (Scotland) legislation.
- Deletion of confidential or sensitive non-personal data to avoid breach of confidence, breach of contract, or commercial damage.
- Deletion of software which is under licence to avoid breach of licences.

2. Scope

- This policy should be applied to all ICT equipment including:
- desktop PCs, laptops, tablets, smartphones and any other portable device.
- Portable storage media including flash drives, DVDs, CDs, tapes.
- Any device that has internal memory or storage including multifunction devices and printers.

3. Disposal of IT Equipment and Digital Media

3.1. No IT equipment or digital media (including portable devices) may be disposed of other than by Corporate Services via the processes set out in this policy.

3.2. All equipment owners should make sure that data which is covered by the data retention schedule is moved to another location before passing equipment to Corporate Services for disposal.

3.3. All IT equipment and digital media must be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Directive.

3.4. IT equipment and digital media should be disposed of by third party contractors on behalf of WWHC. They must adhere national waste and security standards and provide certificates of destruction and copies of waste consignment notes. Appropriate certifications include BS EN15713 Secure Destruction of Confidential Material, ISO 27000 Information Security Management, or other recognised standard.

3.5. Corporate Services staff will keep the "disposal of IT assets" register up to date.

3.6. A certificate of secure destruction will be retained.

4. Equality and Diversity

We are committed to ensuring equal opportunities and fair treatment for all people in our work. In implementing this Policy, we will provide a fair and equal service to all people, irrespective of factors such as gender, race, disability, age, sexual orientation, language or social origin, or other personal attributes.

5. Policy Review

5.1. This policy will be reviewed every 5 years unless there is a requirement to review outwith this cycle.

5.2. The next policy review will be due September 2027.

Equality and Diversity Compliant	Yes
Equality Impact Assessment required	No
Data Protection (GDPR) compliant	Yes
Health & Safety compliant	Yes
Training requirements	None

Regulatory Framework Assurance Information Bank Updated	Regulatory Standard 1: The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users Regulatory Standard 2: The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities. Regulatory Standard 3: The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay. Regulatory Standard 4: The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose.
Policy Implementation	
Reporting arrangements	An annual report for disposed assets should be prepared for the audit.
Policy register updated	
Published on Website	
Publicity material issued	N/A
Related Policies	Risk Management Information Security Management System Privacy Policy

Appendix A

Types of media and methods of destruction.

Item	**Risk**	**Method of Destruction**	**Reasoning**
PCs and Laptops	Medium	Digital file shredding	Low risk of sensitive data being stored locally
Servers	High	Digital file shredding Physical destruction Certificate of destruction required.	High volume of data High risk of sensitive data being stored
Portable Devices	Medium	Digital file shredding	Medium risk of sensitive data being stored
Mobile Phones	Medium	Digital file shredding Reset to factory default Physical destruction	Medium risk of sensitive data being stored (e.g. in emails)
Multi-function devices, printers	Medium	Certificate of data destruction from supplier required.	

Multi-Function Devices and Printers

Photocopiers and printers have hard disks on which electronic copies of documents which have been photocopied, printed or scanned are stored during the operation of the device. Such hard disks must have their data removed by either data wiping or physical destruction which is dependent upon the level of risk associated with the device when it is decommissioned. As part of the contractual arrangements with suppliers, WWHC is provided with proof of data destruction when the device is returned on termination of the lease.

Smart Phones

All smart phones must have their data removed by being reset to factory default or by physical destruction dependent on the level of risk associated with the device and the data it has held when the device is decommissioned. If a device cannot be reset to factory default due to hardware malfunction then it must be physically destroyed.

Portable Media
Portable media which has, or had in the past, contained confidential and personal data should be disposed of in accordance with the above table.