West Whitlawburn
Housing Co-operative

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

Policy Name	**Computer Use Policy**
Policy Author	**Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**September 2025**
Latest date of Next Review	**September 2028**

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.

1. Introduction

1.1. This policy provides guidance on what is considered acceptable use of WWHC's ICT systems. The policy protects individual users, WWHC equipment and data and minimises risk by providing clarity on the behaviours expected. It sets out a framework on how to conduct WWHC business to meet legal, contractual and regulatory requirements and defines how individuals must behave in order to comply with this policy.

2. Purpose

2.1. To make sure that individuals understand their responsibilities for the appropriate use of information technology resources. Understanding what is expected will help individuals to protect themselves, colleagues and WWHC's equipment, information and reputation and ensure that there is clear accountability.

3. Scope

3.1. The policy applies to all staff, volunteers, contractors and their agents (hereafter referred to as individuals) who have access to WWHC networks, equipment and data.

3.2. All WWHC equipment and information (all information systems, hardware, software and channels of communication, including voice- telephony, social media, video, email, instant messaging, internet and intranet). User's personal information which is processed by WWHC equipment is also subject to this policy.

4. General conditions of use

4.1. Before using WWHC equipment or information, individuals must confirm that they agree to comply with this policy and understand that breaching this policy may result in disciplinary procedures and legal action.

4.2. Individuals are responsible and accountable for their actions on the network and must comply with the code of conduct, terms and conditions of employment, and all UK legislation.

4.3. All individuals:

- will use information, systems and equipment in line with WWHC security and Information Management policies.
- should immediately report any breach or suspected breach of this policy to their line manager
- should never undertake illegal activity, or any activity that would be harmful to WWHC's reputation or jeopardise staff and/or stakeholders data.

- should understand that both business and personal use of WWHC systems will be monitored as appropriate.
- should understand that they can use whistleblowing procedures if it is believed that someone is misusing WWHC assets, information or electronic equipment.
- will undertake education and awareness on security and using WWHC information and technology, in order to support the understanding of recognising and reporting threats, risks, vulnerabilities and incidents.

4.4. Harassment (including sexual), intimidation or abuse of employees using WWHC devices, accounts, systems, software or hardware will not be tolerated. Similarly, harassment (including sexual), intimidation or abuse of employees by third parties who use any form of technology to interact with WWHC will not be tolerated. Individuals suspected to be in breach of this will be subject to the Disciplinary and Grievance Policy (or otherwise for as per the Unacceptable Actions Policy).

5. Use of Individual User Accounts

5.1. All employees are provided with a username and password specific to them. They are accountable for all activity undertaken using their user account name. Individuals must not:

- Allow anyone else to use their username and password.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's username and password to access WWHC's IT systems.
- Leave passwords unprotected (for example writing it down).
- Perform any unauthorised changes to WWHC's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-WWHC authorised device to the WWHC network or IT systems.
- Store WWHC data on any non-authorised WWHC equipment.

- Give or transfer WWHC data or software to any person or organisation outside WWHC without the authority of WWHC.

6. Managing and protecting information

6.1. Individuals must understand that they and WWHC have a legal responsibility to protect personal and sensitive information and must not misuse their position to further private interests or those of others.

6.2. Individuals should make sure that all information is created, used, shared and disposed of in line with business need and in compliance with the Information Security Management System, Disposal of IT Equipment, and other relevant policies.

6.3. Individuals must not attempt to access anyone's personal data unless there is a legitimate business need that is appropriate to their job role.

6.4. Individuals must not provide information in response to any type of request without validating the source of the request is legitimate.

6.5. Individuals must not attempt to access, amend, damage, delete or disseminate files, emails, communications or data without the appropriate authority.

7. Personal Use

7.1. The networks are provided for business use. Personal use is permitted in an employee's own time, i.e. when not "clocked in", where such use does not affect the individual's business performance, is not detrimental to WWHC in any way, not in breach of any term and condition of employment and does not place the individual or WWHC in breach of statutory or other legal obligations.

8. Clear Desk and Clear Screen Policy

8.1. In order to reduce the risk of unauthorised access or loss of information WWHC enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

9. Working Off-site

9.1. The following controls must be applied:

- Working away from the office must be in line with WWHC Homeworking policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- Working from an internet cafe is not permitted.
- Staff are not permitted to use their personal laptops or other devices to access WWHC servers remotely.
- Staff may use their personal devices (e.g. mobile phone or laptop) to access their work email account. Once the work or task is complete staff must ensure to log out of all work-related platforms.

10. Mobile Storage Devices

10.1. Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only WWHC authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

11. Software

11.1. Employees must use only software that is authorised by WWHC on WWHC's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on WWHC computers must be approved and installed by WWHC's Managed Service Provider (MSP).

12. Viruses

12.1. The MSP has implemented centralised, automated virus detection and virus software updates within the WWHC. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

a. Remove or disable anti-virus software.
b. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved WWHC anti-virus software and procedures.

13. Actions upon Termination of Contract

13.1. All WWHC equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to WWHC at termination of contract.

13.2. All WWHC data or intellectual property developed or gained during the period of employment remains the property of WWHC and must not be retained beyond termination or reused for any other purpose.

13.3. Staff email accounts will be retained for a 6 week period after their final working day. After this period the account will be deleted by WWHC's MSP as instructed by the Corporate Services Officer or the Deputy Director.

14. Monitoring and Filtering

14.1. All data that is created and stored on WWHC computers is the property of WWHC and there is no official provision for individual data privacy, however wherever possible WWHC will avoid opening personal emails.

14.2. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. WWHC has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

14.3. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the

Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

15. 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.

16. Policy Review

16.1. This policy will be reviewed every 3 years unless there is a requirement to review out with this cycle.

Equality and Diversity Compliant	Yes
Equality Impact Assessment required	No
Data Protection (GDPR) compliant	Yes
Health & Safety compliant	Yes
Training requirements	Annual refresher training for all staff and volunteers.
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. Regulatory Standard 5: The RSL conducts its affairs with honesty and integrity

Policy Implementation	
Reporting arrangements	None
Policy register updated	
Published on Website	
Publicity material issued	N/A
Related Policies	Standing Orders Risk Management Information Security Management System Disposal of IT Equipment Code of Conduct

Equalities Impact Assessment

Policy/Project/Service Information			
Lead Officer	Corporate Services Officer		
Policy / Project / Service	Computer Use	**New Policy / Project / Service or revision of existing?**	Revision of Existing
Is this a reassessment following amendments being required at a previous assessment?	No		
Briefly describe the aims, objectives and purpose of the policy / project / service.	Provide guidance on what is considered acceptable use of WWHC IT systems and assets. The Computer Use policy is implemented to ensure that individuals understand their responsibilities for the appropriate use of information technology resources. Understanding what is expected will help individuals to protect themselves, colleagues and WWHC's equipment, information and reputation and ensure that there is clear accountability.		
Who is intended to benefit from the policy / project / service? (E.g. applicants, tenants, staff, contractors)	Staff, tenants, members, applicants, contractors, all other stakeholders. WWHC Management Committee and the organisation's reputation and assets		
What outcomes are wanted from this policy / project / service? (E.g. the	To ensure the security of all WWHC owned or processed data and to ensure that staff understand what is acceptable regarding WWHC IT systems. To ensure security to all employees, tenants, members,		

measurable changes or benefits to members/ tenants / staff)	applicants, contractors and other stakeholders personal and sensitive data.

Consultation
Who have you engaged and consulted with as part of your assessment? Change identified through review of Dignity at Work Policy (sexual harassment updates). Staff participation on risk assessment.

Equalities Impact Assessment			
Which protected characteristics could be affected by the policy, practice, or service?		**Identify any positive impact/s that could result for each of the protected characteristic groups.**	**Identify any negative impact/s that could result for each of the protected characteristic groups.**
Age			
Disability			
Gender Reassignment			
Marriage & Civil Partnership			
Race			
Religion/Belief			
Pregnancy/Maternity			
Sex			
Sexual Orientation			

Action Plan To Mitigate Negative Impact		
What action/s are required to address the impacts arising from this assessment?		
Protected characteristics	Action	Implementation Date
Age		
Disability		
Gender Reassignment		
Marriage & Civil Partnership		
Race		
Religion/Belief		
Pregnancy/Maternity		
Sex		
Sexual Orientation		
Human Rights		

Final Decision	Tick relevant box	Include explanation where appropriate
Approved for implementation without change		
Amend or change the Policy/Project/Service		

Continue the Policy/Project/Service without change (despite impact)		
Stop the Policy/Project/Service		
Lead Officer Signature	R.Hosie	
Date	11/09/2025	
Date approved by Management Committee/ Sub Committee	30/09/2025	