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

Policy Name	**ICT, Internet and Email Use Policy**
Policy Author	**Data Protection Officer / Corporate Services Officer**
Approved by Sub Committee	**N/A**
Approved by Management Committee	**March 2026**
Latest date of Next Review	**March 2029**

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 WWHC and Community Benefit Societies Act 2014

1 Introduction

1.1 This Policy outlines the principles and standards which West Whitlawburn Housing Co-operative (WWHC) requires those using its information and communications technology (ICT) facilities, including the Internet, e-mail and other communications systems, to observe. It also explains when WWHC will monitor the use of those facilities and the action WWHC will take if the terms of this Policy are breached.

1.2 WWHC expects all its ICT facilities to be used in an effective and professional manner and requires all staff to do so. These facilities are provided by WWHC for its own business purposes to assist its staff in carrying out their duties effectively. It is the responsibility of all staff to ensure that ICT facilities are used for proper business purposes and in a manner that does not compromise WWHC in any way.

1.3 Professional integrity is central to WWHC, and it must characterise all its dealings. All staff should think about how their own image, or that of WWHC, may be affected by how they use WWHC's ICT facilities. The same professional ethical obligations apply to conduct in online and offline environments. As such, staff must comply with the Code of Conduct throughout all interactions carried out using any of WWHC's ICT facilities.

1.4 This Policy applies to the use of WWHC's ICT facilities while at work and when using WWHC's technology from outside work (e.g. when accessing WWHC's facilities remotely using a WWHC issued laptop or smartphone).

1.5 Misuse of WWHC's ICT facilities can expose both staff and WWHC to legal or financial liability. For example, staff may breach copyright or licensing arrangements, incur liability for defamation or harassment or introduce viruses or expose the ICT facilities to other security threats, such as hacking and ransomware attacks. This Policy is designed to safeguard WWHC from such liabilities. It is important that all staff read the Policy carefully and ensure that all use of WWHC's ICT facilities is in accordance with its terms.

1.6 This Policy applies to all staff of WWHC, agency workers, volunteers, consultants and other contractors and Committee members (as if they were staff of WWHC), who have access to WWHC's ICT facilities as part of their roles or work with WWHC. It also applies to the limited permitted personal use of WWHC's ICT facilities by the same persons.

1.7 This Policy does not form part of any employee's contract of employment and WWHC may amend it at any time.

1.8 The Data Protection Officer (DPO) and Corporate Services Officer are responsible for the monitoring and implementation of this Policy. Any questions about the content or application of this Policy or other comments should be referred to them.

2 Use of WWHC's ICT facilities

2.1 Staff may use WWHC's ICT facilities only to the extent that they are authorised to do so. Staff should not use WWHC's ICT facilities for any purpose that is not connected to WWHC's business, unless they have express permission to do so or they are making personal use of the ICT facilities as permitted by this Policy (see paragraph 9).

2.2 Use of WWHC's ICT facilities for commercial purposes, other than the business of WWHC, is strictly prohibited.

2.3 Staff with access to WWHC's network must adhere to strict access controls to reduce the risk of virus infections, hacking and other unauthorised access attempts:

2.3.1 only authorised equipment is allowed to connect to WWHC's network

2.3.2 remote access is also restricted to authorised equipment and access must only be via secure means; and

2.3.3 access via unauthorised equipment is prohibited.

2.4 WWHC licenses software from a number of sources. WWHC does not own that software and must comply with any restrictions or limitations on use in accordance with its licence agreements. All staff must adhere to the provisions of any such software licence agreements.

2.5 Staff must not use any software for any purpose outside the business of WWHC without express permission of the Director or as otherwise permitted by the terms of this Policy.

2.6 Staff must not copy, download or install any software without first obtaining permission from WWHC's Managed Service Provider and the Corporate Services Officer.

3 Confidentiality

3.1 E-mail and the Internet are not secure means of communication, and third parties may be able to access or alter messages that have been sent or received.

3.2 E-mails containing matters of a sensitive or confidential nature should be clearly marked in the subject header as such. Any attachments containing sensitive or confidential information should be password-protected, with the password transmitted to the recipient of the e-mail by another means (e.g. text message, telephone call or separate email).

4 General rules regarding communications and e-mail

4.1 All communications, including e-mail, should always reflect the highest professional standards. All staff must:

4.1.1 keep messages brief, factual and to the point, avoiding matters of personal opinion at all times

4.1.2 ensure that spelling and grammar are carefully checked before sending

4.1.3 ensure that all e-mails sent from WWHC include the current confidentiality disclaimer

4.1.4 ensure that all e-mails sent from WWHC include their signature

4.1.5 ensure that the content and origin of e-mails is accurate, and that names or affiliations within e-mails are not concealed or misrepresented and the source is not altered

4.1.6 ensure that an appropriate heading is inserted in the subject field (including a confidentiality or sensitivity indicator, if appropriate); and

4.1.7 double check the recipient(s) before pressing the send button. Not only can it be embarrassing if an e-mail is sent to the wrong person, but it can also result in the unintentional disclosure of confidential information about WWHC or a service user in breach of data protection legislation.

4.2 Staff must not send messages from another person's e-mail address (unless authorised in the proper performance of their duties) or under an assumed name.

4.3 Staff must use appropriate etiquette and must not send offensive, demeaning, disruptive or defamatory messages or images by any method. This includes any sexist or racist material or any material which could be offensive on the grounds of a person's disability, physical appearance, age, sexual orientation, gender or religion or beliefs.

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 of being in breach of this will be subject to the Disciplinary and Grievance Policy (or otherwise as per the Unacceptable Actions Policy).

4.5 Staff must not download, send, receive or forward any message or image which could be regarded as personal, potentially offensive or frivolous to any recipient or to any other person (even if not sent to them), including messages containing political communications.

4.6 If staff receive any communication containing material that is offensive or inappropriate to the office environment, staff must delete it immediately. Under no circumstances should such communication be forwarded either internally or externally, other than internally to the DPO or their line manager to report a breach of this Policy.

4.7 Staff should not transmit anything in an e-mail or other communication that they would not be comfortable writing (or someone else reading) in a letter. E-mails leave a retrievable record and, even when deleted, can remain on both the staff member's computer and on WWHC's ICT facilities back-up system. E-mails can be recovered and used as evidence in court proceedings and / or reviewed by regulators and may be made available to the subject of the e-mail following a request made under data protection legislation.

4.8 Staff must not send trivial messages or copy or forward messages to recipients who do not need to receive them, or send or forward chain mail, junk mail, cartoons, jokes or gossip.

4.9 Staff must only use a WWHC e-mail address for sending and receiving work-related e-mails and must not use their own personal e-mail accounts to send or receive e-mails for the purposes of WWHC's business. Staff must not send (inside or outside work) any message in WWHC's name, unless it is for an authorised, work-related purpose.

4.10 Staff must not send unsolicited commercial e-mails to persons with whom they do not have a prior relationship without the express permission of their line manager.

5 Passwords and security

5.1 Staff are personally responsible for the security of all ICT equipment allocated to or used by them. Staff must not allow ICT equipment allocated to them to be used by any other person other than in accordance with this Policy. Laptops may be shared occasionally (i.e. when a staff member has forgot to bring their device for an online meeting) but staff must utilise their individual login and password when accessing systems.

5.2 Staff must use passwords on all ICT equipment allocated to them and must keep any password allocated to them confidential and must change their password regularly, or as enforced by WWHC's software providers or Managed Service Provider (MSP).

5.3 Staff may not use another staff member's username and / or password to access WWHC's ICT facilities, nor may staff allow any other person to use their password(s). If it is anticipated that access is required to a staff member's confidential files in their absence, the files should be copied to a network location that is properly secure where access can be obtained.

5.4 All staff must log out of WWHC's ICT facilities or lock their computer when leaving their desk for any period of time. All staff must log out and shut down their computer at the end of the working day, unplugging the power cable or extension(s) from the wall.

6 Contact lists

6.1 Lists of contacts compiled by staff during their employment and stored on WWHC's e-mail system and / or other of WWHC's database(s) (irrespective of how they are accessed) belong to WWHC. Such lists may not be copied or removed by staff for use outside their employment or after their employment with WWHC ends.

7 Systems and data security

7.1 Be vigilant when using WWHC's e-mail system. Computer viruses are often sent by e-mail and can cause significant damage to WWHC's ICT facilities. Be particularly cautious in relation to unsolicited e-mail from unknown sources.

7.2 If staff suspect that an e-mail may contain a virus, they should not reply to it, open any attachments to it or click on any links in it and must contact the Corporate Services Officer or IT Support Team immediately for advice.

7.3 No personal computer, mobile phone, tablet computer, USB storage device or other device is permitted to be connected to WWHC's ICT facilities or network without express prior permission from Corporate Services Officer or IT Support Team.

7.4 Staff must not run any '.exe' files, particularly those received via e-mail, unless authorised to do so in advance by Corporate Services Officer or IT Support Team. Unauthorised files should be deleted immediately upon receipt without being opened.

7.5 Staff must not access or attempt to access any password-protected or restricted parts of WWHC's ICT facilities for which they are not an authorised user.

7.6 All staff must inform WWHC's IT Support Team immediately if they suspect their computer may have a virus and must not use the computer again until informed it is safe to do so.

7.7 WWHC implement centralised, automated virus detection and virus software updates within its ICT environment. All PCs and laptops have antivirus software installed to detect and remove any virus automatically.

7.8 Staff must not remove or disable anti-virus software, nor should they attempt to remove virus-infected files or clean up an infection. Staff must contact the IT Support Team who will carry out these actions if required.

7.9 All laptop, smartphone and mobile phone users should be aware of the additional security risks associated with these items of equipment. All such equipment must be locked away in a secure location if left unattended overnight.

7.10 Working from an internet café or other public meeting space (e.g. Public Library, Co-working space etc.) is not permitted as WWHC cannot guarantee the security of the location or network(s).

8 The Internet

8.1 Access to the Internet during working time is primarily for matters relating to WWHC's business. Reasonable, limited personal use of the Internet is permitted in accordance with paragraph 9.

8.2 Any unauthorised use of the Internet is strictly prohibited. Unauthorised use includes (but is not limited to):

8.2.1 creating, viewing, accessing any webpage or posting, transmitting or downloading any image, file or other information unrelated to WWHC's business and which could be regarded as pornographic, illegal, criminal, offensive, obscene, in bad taste or immoral and / or which is liable to cause embarrassment to WWHC or to WWHC's service users.

8.2.2 engaging in computer hacking and / or other related activities; and

8.2.3 attempting to disable or compromise security of information contained on WWHC's ICT facilities or those of a third party.

8.3 Staff are reminded that such activity may also constitute a criminal offence.

8.4 Postings placed on the Internet may display WWHC's address. For this reason, before posting information, staff should ensure that the information reflects the standards and policies of WWHC. Under no circumstances should information of a confidential or sensitive nature be placed on the Internet. Staff must not use WWHC's name in any Internet posting (inside or outside work), unless it is for a business purpose and agreed by your line manager beforehand.

8.5 Information posted or viewed on the Internet may constitute published material. Therefore, reproduction of information posted or otherwise available over the Internet may be done only by express permission from the copyright holder. Staff must not act in such a way as to breach copyright or the licensing conditions of any Internet site or computer program.

8.6 Staff must not commit WWHC to any form of contract through the Internet without the express permission of their line manager.

8.7 Subscriptions to news groups, mailing lists and social networking websites using WWHC's ICT facilities are permitted only when the subscription is for a business purpose. Any other subscriptions are prohibited.

8.8 WWHC may block or restrict access to any website at its discretion.

9 Personal use of WWHC's ICT facilities

9.1 Reasonable personal use of WWHC's facilities to send personal e-mail, browse the Internet and make personal telephone calls is allowed, if it does not interfere with the performance of a staff member's duties and the terms of this Policy are strictly adhered to. WWHC reserves the right, at its absolute discretion, to withdraw this privilege at any time and/or to restrict access for personal use.

9.2 Personal use must meet these conditions (in addition to those set out elsewhere in this Policy):

9.2.1 personal use must be minimal (both in terms of time spent and frequency) and reasonable and must take place exclusively outside normal working hours, i.e. during lunch or other breaks, or before and after work.

9.2.2 personal use must not affect the performance at work of any member of staff or otherwise interfere with WWHC's business; and

9.2.3 personal use must not commit WWHC to any costs (e.g. WWHC's telephone system may not be used for premium rate or international calls, unless this is necessary for WWHC's business or is expressly authorised by your line manager).

9.3 WWHC does not permit access to web-based personal e-mail, such as Hotmail, Yahoo!, Outlook.com or Gmail, on its ICT facilities at any time, due to the additional security risks presented by their use.

10 Lost, Stolen or Damaged ICT Equipment

10.1 Staff must report any lost, stolen or damaged ICT equipment issued to them to their line manager and the Corporate Services Officer as soon as possible. Such devices may contain business data and appropriate steps must be taken to minimise the risk to WWHC and other data subjects.

10.2 In the event of a lost or stolen device, the IT Support Team must be notified with a request to carry out a factory reset remotely.

11 Actions Upon Termination of Employment

11.1 Staff must return all WWHC equipment and data (e.g. laptops, smartphones, USB memory devices, CDs/DVDs) when their employment ends.

11.2 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 contract termination or re-used for any other purpose.

11.3 Staff accounts used to access systems, and software will be blocked by the end of their final working day to prevent any unauthorised access beyond their employment. This will be instructed or actioned by the Corporate Services Officer in the first instance. In their absence, the employee's line manager will be responsible for this.

12 Monitoring

12.1 WWHC's ICT facilities enable WWHC to monitor telephone, e-mail, Internet and other communications (including mobile phone use). Staff member's use (including personal use) of WWHC's ICT facilities may be monitored for business reasons, to carry out WWHC's obligations as an employer and to monitor compliance with the terms of this Policy.

12.2 WWHC reserves the right to monitor, intercept, retrieve and read the contents of any internal or external e-mail or other communication, to record any telephone conversation or to check Internet usage (including pages visited and searches made) as reasonably necessary in the interests of WWHC's business, including for these purposes (the list is not exhaustive):

12.2.1 to establish facts.

12.2.2 to establish compliance with regulatory or self-regulatory procedures.

12.2.3 to prevent, detect or investigate alleged crime or wrongdoing.

12.2.4 to investigate or detect the unauthorised use of WWHC's ICT facilities or to ascertain compliance with WWHC's policies, practices or procedures (including this Policy).

12.2.5 to locate and retrieve lost messages or files.

12.2.6 to check whether communications are relevant to the business (for example, when staff are absent due to sickness or annual leave – in these circumstances, it may be unavoidable that some private messages will be read or heard); and / or

12.2.7 to comply with any legal obligation.

13 Prohibited use and breach of this Policy

13.1 WWHC considers this Policy to be extremely important. Breach of this Policy may be considered gross misconduct and therefore actioned in line with the Disciplinary and Grievance Policy. In addition, or as an alternative, WWHC may withdraw or restrict a staff member's Internet and / or e-mail access.

13.2 Examples of matters that will usually be treated as gross misconduct include (this list is not exhaustive):

13.2.1 unauthorised use of the Internet as outlined in paragraph 8.2 above.

13.2.2 creating, transmitting or otherwise publishing any false and defamatory statement about any person or organisation.

13.2.3 creating, viewing, accessing, transmitting or downloading any material which is discriminatory or may cause embarrassment to other persons.

13.2.4 accessing, transmitting or downloading any confidential information about WWHC and / or any Co-operative staff and / or service users, except where authorised in the proper performance of duties;

13.2.5 accessing, transmitting or downloading unauthorised software; and

13.2.6 viewing, accessing, transmitting or downloading any material in breach of copyright.

13.3 Staff may also be personally liable for their actions if their conduct is unlawful and constitutes a crime.

14 Equalities

14.1 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.

15 Review and training

15.1 WWHC regularly monitors the effectiveness of this Policy to ensure it is working in practice and will review and update this Policy as and when necessary.

15.2 WWHC will provide information and/or training on this policy at induction and refresher training periodically.

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

Equalities Impact Assessment

Policy/Project/Service Information			
Lead Officer	Corporate Services Officer		
Policy / Project / Service	ICT, Internet and Email Use Policy	**New Policy / Project / Service or revision of existing?**	Revision of existing – Computer Use Policy
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.	Outlines the principles and standards which WWHC requires those using its ICT facilities and other communications technology. Further explains WWHC's approach to monitor such ICT facilities.		
Who is intended to benefit from the policy / project / service? (E.g. applicants, tenants, staff, contractors)	Anyone who has access to WWHC's ICT facilities. Also, Management Committee to ensure a responsible and accountable organisation.		

What outcomes are wanted from this policy / project / service? (E.g. the measurable changes or benefits to members/ tenants / staff)	To safeguard WWHC from any liabilities (IT threats, copyright breach, defamation, harassment, other hacking etc.)

Consultation
Who have you engaged and consulted with as part of your assessment? Model Policy provided by DPO – reviewed alongside Computer Use and passed to senior staff team for feedback.

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	27/02/2026
Date approved by Management Committee/ Sub Committee	27/04/2026