Information and Communication Technology (ICT) Acceptable Use Policy

Status: Approved

Policy Lead :	Russell Phillips – ICT & Digital Transformation Lead
Owned By :	Russell Phillips – ICT & Digital Transformation Lead
Date Approved:	May 2025
Approved By :	Operations Committee
Review Date:	May 2028
Regulatory / Legislative Considerations/ References	N/A
Other Documents to be read in conjunction with this policy :	N/A

Berwickshire Housing Association is a Registered Society. Registration No.: SP2482RS
Scottish Charity No.: SC042342 Registered Office: 55 Newtown Street, Duns, TD11 3AU

Policy Title:	**Information and Communication Technology (ICT) Acceptable Use Policy**
Purpose / Aim of policy:	Berwickshire Housing Association is committed to ensuring the responsible and ethical use of its IT resources. This policy establishes guidelines to safeguard the security, confidentiality, and integrity of information, as well as to maintain the optimal performance of IT systems.
Scope of Policy:	This policy outlines the rules and guidelines for the appropriate use of information technology resources within Berwickshire Housing Association. The policy applies to all employees, contractors, and third-party entities who have access to the organisation's IT infrastructure and systems.
Definitions:	• Acceptable use of IT refers to the appropriate and permitted ways to utilise an organisation's information technology resources, such as computers, networks, software, and data. It outlines the boundaries of appropriate behaviour when accessing and using these resources, ensuring they are used for legitimate purposes, in compliance with policies, and with respect for others. • Computer Security, also known as cybersecurity, refers to the measures and practices used to protect computer systems, networks, and data from unauthorized access, theft, damage, or disruption. • Computer Hardware refers to the physical, tangible parts of a computer system. These include components like the CPU, RAM, hard drive, motherboard, and peripherals like monitors, keyboards, and mice. • Computer software, also known as programs or applications, refers to the set of instructions that tell a computer how to perform specific tasks • Electronic Messaging Platforms are systems that enable users to send and receive messages, including text, multimedia, or voice, over the internet or a network. • Internet Access is the ability to connect to the internet, enabling users to browse websites, send emails, and access various online services. • Social Media refers to websites and applications that focus on communication, community-based input, interaction, content-sharing and collaboration
Specific detail related to each strand in the scope:	• Computer Security • Computer Hardware • Computer Care • Electronic Messaging Platforms • Internet Access • Mobile Phone And Mobile Device Usage • Social Media Policy
Approval Source:	Operations Committee

Equality Impact Assessment:	N/A
Glossary of Terms	• BHA - Berwickshire Housing Association • One Drive - a private cloud-based folder • Phishing - the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. • DocMan a third party Electronic Document and Records Management platform
Risk Implications:	• Misuse of IT • Theft of device • Loss of data • Cyber Security Breach • Misrepresentation of BHA • Reputational damage

1. INTRODUCTION

This policy outlines the rules and guidelines for the appropriate use of information technology resources within Berwickshire Housing Association . The policy applies to all employees, contractors, and third-party entities who have access to the organization's IT infrastructure and systems.

2. POLICY AIMS AND OBJECTIVES

Berwickshire Housing Association is committed to ensuring the responsible and ethical use of its IT resources. This policy establishes guidelines to safeguard the security, confidentiality, and integrity of information, as well as to maintain the optimal performance of IT systems.

3. COMPUTER SECURITY

3.1. The ICT facilities can only be accessed using your personal login and password. The use, or attempted use, of a login, other than your own, that has not been authorised by your line manager will be investigated and could result in disciplinary action being taken.

3.2. You must keep your personal password confidential, and it must meet the Association's minimum password security criteria. If you suspect that your password has been discovered, or that you have accidentally given it away in a phishing attempt, inform the ICT Team and change it immediately. Before leaving your computer unattended you should make sure that you lock it.

3.3. When a laptop is provided to you, it is your sole responsibility to ensure you take all measures necessary to prevent loss of the equipment and subsequent loss of data.

3.4. Personal Data or Commercially sensitive information must never be copied onto removable media such as a Portable hard drive, USB Stick or CD/DVD/BluRay disk without the permission of the ICT Team. If you need to send data or similar to an external organisation, check with the ICT team before doing so.

3.5. Personal Data or Commercially sensitive information must never be copied to an online file sharing site without the permission of the ICT Team. If you need to send data or similar to an external organisation, check with the ICT team before doing so.

3.6. All working documents must be stored on the file server or in DocMan or in SharePoint or in your BHA supplied One Drive. A private drive is provided on the file server and a private One Drive is provided for your use and is visible only to you. You must never save work on your desktop or C: drive. If you cannot connect to the server for any reason and have to save files on your C:/ drive you should move them back to the server as soon as possible and delete any duplicate files from your C:/ drive.

3.7. Controlled documents must only ever be accessed and saved back to the intranet.

4. COMPUTER SOFTWARE

4.1. Only software provided/approved by ICT may be used on BHA's computer equipment.

4.2. The introduction of unauthorised software, including programs and data, increases the risk of a virus being introduced, with potentially disastrous results. This includes computer games. Playing games on Group equipment is strictly forbidden.

4.3. BHA have an automatically applied default organization branded Windows background, lock screen and user profile image to prevent screen glare, and to make reading of screen icons easier for staff with dyslexia or colour blindness. This also prevents staff choosing a background, lock screen or profile image that could be deemed upsetting or offensive to others. However, if a member of staff replaces these images for any reason with an image that could be deemed upsetting or offensive to others, BHA reserves the right to ask you to remove those images at any time.

4.4. Making unauthorised copies of software licensed to BHA is not permitted. Software is protected by copyright and copying is a criminal offence.

5. COMPUTER HARDWARE

5.1. To minimise accidental damage to computer hardware, it must only be serviced by the ICT team or a recognised Service Agent.

5.2. Use of BHA's equipment for personal matters is permitted within reason.

6. COMPUTER CARE

You must treat the computer equipment with care, especially with regard to food and drink spillage. If you are provided with a portable device, always use the case/cover provided when transporting the equipment.

7. ELECTRONIC MESSAGING PLATFORMS

7.1. Introduction

7.1.1. Use of any BHA messaging platform should be in accordance with APPENDIX 2 - SOCIAL MEDIA POLICY.

7.1.2. General messages to wider groups should be broadcast on MS Teams.

7.1.3. Confidential information must not be sent externally by email without express authority and personal data must never be emailed from unsecured/unencrypted mail systems.

7.2. Legal Action Against BHA

7.2.1. Inappropriate content or comments in messages sent through the email system can give rise to legal action against BHA. Email messages should be treated like any other form of correspondence as these are subject to disclosure in the event of a Subject Access Request.

7.3. BHA's Rights

7.3.1. BHA reserves the right to retrieve the contents of messages for the purpose of monitoring whether the use of the email system or Teams is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts or to comply with any legal obligation. This access can only be authorised by two members of the Executive Team.

7.3.2. BHA will not routinely monitor messages but is required to keep logs of all messages sent and received for a period of three years.

7.4. Security

7.4.1. If you are given access to the email system you are responsible for the password and access security in line with section 1. COMPUTER SECURITY.

7.5. General Rules

7.5.1. Should you receive an email which has been wrongly delivered to your email address you should notify the sender of the message by replying to the email. You should not disseminate, distribute forward, copy, print the email or disclose any information within the email and permanently delete the message from your system and devices.

7.5.2. Should you receive an email which contravenes this policy the email should be forwarded to the ICT Team.

7.5.3. If you receive an email with an attachment and you have any doubts about its origin or contents, do not open it as it may contain a virus. Report the email to the ICT Team immediately.

7.5.4. Misuse of the email system in breach of this policy may lead to disciplinary action.

7.5.5. Misuse of the email system by transmission of any material that is deemed to be defamatory, offensive, obscene, untrue, malicious, of a political nature or in breach of copyright could constitute gross misconduct.

8. INTERNET ACCESS

8.1. Introduction

8.1.1. These guidelines are intended to help you make the best use of any Internet resources at your disposal. You should understand the following.

8.1.2. BHA provides Internet access to staff to assist them in carrying out their duties for BHA. Internet access is provided as a business tool, and although occasional personal usage is permitted, it should only be outside normal working hours or when on an official break from work such as lunchtime. You must not view any content that is defamatory, offensive, obscene, untrue, and malicious or breaches copyright (for example, downloading media files from a file sharing website). As such the following categories of website are blocked for your protection:

Adult / Mature Content	**Potentially Liable**
Alcohol	Child Sexual Abuse
Alternative Beliefs	Crypto Mining
Dating	Discrimination
Gambling	Drug Abuse
Lingerie and Swimsuit	Explicit Violence
Marijuana	Extremist Groups
Nudity and Risqué	Hacking
Other Adult Materials	Illegal or Unethical
Pornography	Plagiarism
Sports Hunting and War Games	Potentially Unwanted Program
Tobacco	Proxy Avoidance
Weapons (sales)	Terrorism

Bandwidth Consuming
None

General Interest - Business
Cryptocurrency
General Interest - Personal
Advertising
Brokerage and Trading
Domain Parking
Folklore
Games
Meaningless Content

Security Risk
Dynamic DNS
Malicious Websites
Newly Observed Domain
Newly Registered Domain
Phishing
Spam URL's

8.1.3. When using BHA's Internet access facilities you should comply with the following guidelines.

8.2. DO

- Do keep your use of the Internet to a minimum
- Do check that any information you access on the Internet is accurate, complete and current.
- Do check the validity of the information found.
- Do respect the legal protections to data and software provided by copyright and licenses.
- Do inform ICT immediately of any unusual occurrence.

8.3. DO NOT

- Download text or images which contain material of a pornographic, racist, or extreme political nature, or which incites violence, hatred or any illegal activity.
- Stream online content that is not work related.
- Do not download content from Internet sites unless it is work related.
- Do not use BHA's computers to make unauthorised entry into any other computer or network, and do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse Act 1990.
- Do not represent yourself as another person or act anonymously.
- Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

8.4. Please note the following

8.4.1. All activity on the Internet is monitored and logged.

8.4.2. All material viewed is scanned for viruses.

8.4.3. All the content viewed may be scanned for offensive material.

8.4.4. If you are in any doubt about an issue affecting Internet access you should contact the ICT Team.

8.4.5. Misuse of the Internet facilities could constitute gross misconduct.

APPENDIX 1 - MOBILE PHONE AND MOBILE DEVICE USAGE

1 GENERAL USE

1.1 BHA recognises that in certain circumstances the provision and use of a mobile device is required for business use. The request for a mobile device to be issued will be made on a case-by-case basis by the Line Manager.

2 PERSONAL USAGE

2.1 BHA Mobile Phones are provided for business use. Limited personal use of mobile phones is permitted.

2.2 Monitoring mobile phone data and call usage is in place at BHA to ensure continuity of service. Please note, excessive personal use is captured by default and will be reported to your line manager.

2.3 Employees travelling or away from home may make limited private use of a business mobile phone to ring or text home, where travel arrangements change or family circumstances dictate.

2.4 Where circumstances necessitate the use of BHA's mobile phone for private purposes, the employee to whom the Phone is issued is responsible for ensuring that excessive private use and the associated cost is reimbursed to BHA.

2.5 The loss or theft of a mobile phone must be reported immediately to the ICT Team.

2.6 Where the employee leaves BHA, the mobile phone and any accessories remains the property of BHA. BHA may agree to release the mobile number of a member of staff who is leaving to them for personal use in the future. On such occasions the employee will be liable for any cost associated with doing so.

2.7 Should a former worker fail to return the mobile phone to BHA, they will be held responsible for any calls and line rental incurred until the phone is either returned or disconnected.

3 TERMS OF USAGE

3.1 Employees Responsibilities:

3.1.1 To be used in a safe and controlled manner at all times.

3.1.2 The employee is responsible for taking reasonable precautions to avoid loss or misuse of the mobile phone and any allied equipment. Employees must not leave a mobile phone in an unattended vehicle.

3.1.3 It is the employee's responsibility to use their mobile phone as reasonably required to do so. If calling/texting another member of staff the mobile phone should always be used to take advantage of free or discounted user group calls and texts.

3.1.4 Users who have access to email on their mobile phone also have access to mobile internet services. Users are discouraged from subscribing to any mobile internet service or download any content that is chargeable. Any costs incurred in this situation will be payable by the user.

3.2 BHA's Responsibilities:

3.2.1 A Register of all mobile phones will be held centrally by the ICT Team.

3.2.2 Contracts will be reviewed regularly, and thresholds/plans may be adjusted accordingly.

3.2.3 The Executive Director Business Support will be responsible for the monitoring and reviewing of staff mobile phone bills, ensuring a charge for reimbursement of personal calls is forwarded to the user within 3 months of the cost being incurred.

3.2.4 Mobile devices with in-built Global Positioning Satellite (GPS) sensors may be utilised without notice for a variety of purposes including but not limited to tracking the whereabouts of devices and lone workers.

4 WHILST DRIVING

4.1 It is illegal to use mobile phones whilst driving (see Appendix 1). When driving, BHA advises that phones are switched off.

5 DAMAGE TO MOBILE PHONES

5.1 Mobile phones in need of repair should be handed back to the ICT Team who will return it to the supplier for repair or replacement.

6 PASSWORDS OR PERSONAL IDENTITY NUMBERS (PIN)

6.1 It is a requirement to protect your mobile phone or device with the use of a Password, PIN number or biometric data (fingerprint/Face ID).

APPENDIX 2 - SOCIAL MEDIA POLICY

1 INTRODUCTION

1.1 The internet is a part of our everyday lives and the BHA recognises that it allows us to communicate with our friends, families and colleagues and to connect with the online community

1.2 When you are on the internet your actions could be construed as being representative of BHA. This guidance helps you to protect your privacy and your reputation and ensure everyone is clear about their responsibilities online.

1.3 All we ask of you is that when engaging in social media you are clear about who you are representing, you take responsibility for ensuring that any references to BHA are factually correct and accurate and do not breach our confidentiality policy, and that you show respect for the individuals and communities with which you interact.

2 REPRESENTATION

2.1 BHA understands that your private life is your private life and, as long as it's within the law and doesn't refer to BHA, we're not concerned with what you do online.

2.2 If you decide to associate yourself online with BHA you are taking on additional responsibilities and it's important you are clear about these. You will be representing our brand and you will need to stop and think to make sure you act appropriately.

2.3 You will be representing BHA if you:

2.3.1 Participate in a discussion forum, group or network which relates to BHA (e.g., a Facebook group for your team or BHA);

2.3.2 Talk about BHA;

2.3.3 Upload photos or videos of you in BHA premises or in other ways identified as being associated with BHA, such as giving out your job title;

2.3.4 Are talking to people you work with about events at work or any social event that is associated with BHA or identifies the fact that you are an employee of BHA;

2.3.5 Link your personal social media account to BHA's Corporate Social Media account.

3 RESPONSIBILITY

3.1 If you choose to represent BHA online, you need to act in the same way you do as an employee: responsibly with honesty and integrity. Think about what you are writing. Content on the internet can be seen by people who aren't the intended audience, and once you have written or uploaded something, a copy of it may remain online forever.

3.2 Only disclose publicly available information. You must not comment on or disclose confidential BHA information (such as financial information, future plans, allocation decisions etc). If you require clarification about what BHA information is in the public domain, you should refer to a member of the Executive Team.

3.3 Ensure you do not post material that is obscene, defamatory, threatening, harassing, discriminatory or hateful to another person or entity, including BHA, its employees, its contractors, its partners, its competitors and/or other business-related individuals or organisations.

3.4 If you write about BHA make it clear you are an employee.

4 RESPECT

4.1 Its basic stuff: you shouldn't be rude about colleagues or customers. Its fine to have a Facebook status saying 'you've had a bad day' but think about what you are saying online. Online communication just isn't private. Ask yourself if you would be happy with your family, your manager and your friends reading what you've written?

4.2 Illegal material (words or images) or anything that could be perceived as embarrassing, offensive, harassing, or defamatory to any person or entity should never be posted in a context where you represent BHA. Nor should you post any jokes or derogatory comments related to gender, sexual orientation, race, ethnicity, age, marital status, religion, or any other discriminatory ground.

5 PROTECTING YOUR PRIVACY - SOME HELPFUL IDEAS

5.1 There are some simple things you can do to ensure you protect your privacy online.

5.2 If someone says something which is inappropriate or offensive, use the site's reporting tool to highlight the abuse to the site owner.

5.3 Think carefully about who you allow to become your friend on sites like Facebook. Once you have accepted someone as your friend, they will be able to access information about you, including photographs. You can remove friends at any time, and this action isn't notified to the person you remove (although they may notice that they can't see your profile anymore).

APPENDIX 3 – PERSONALLY OWNED SMARTPHONE POLICY

1. BHA recognises that smartphones are a part of everyday lives and embraces them in its business. It also recognises that they can, if misused, inadvertently, or otherwise, lead to a data breach.

2. Personally owned smartphones can be used to download and sign into any MS Office 365 apps to access your BHA account, but no documents or information should ever be downloaded or saved to a personal device or personal cloud storage accounts.

3. This policy sets out the expectations BHA has of its staff that bring personally owned smartphones into the workplace.

4. Personally owned smartphones are permitted in the workplace but usage during working hours is at the Line Manager's discretion. In all cases personal owned smartphones should not:

   4.1 Be on display in a public facing area of the workplace or be used for any BHA business;

   4.2 Be used to take pictures of any tenants, service users, their family members or their property, even if it is on or within the boundary of a BHA owned home;

   4.3 Be used to take pictures of any documents on behalf of tenants or other service user;

   4.4 Be used to capture screen images of information that is held on BHA's systems;

   4.5 Be connected to any BHA wireless network except BHA-Public.

5. Any breach of this policy could lead to disciplinary action.