IT Acceptable Use Policy

Title	IT Acceptable Use Policy
Purpose	The IT Acceptable Use Policy (AUP) sets out the guidelines for acceptable use of Maryhill Housing's IT systems, hardware and user accounts by authorised users. The policy details what is required to permit secure and efficient use of IT systems, hardware, and user accounts, essential for day-to-day operations and delivery of services to support the Association's work.
Scope	This policy applies to all authorised users of Maryhill Housing and Maryhill Living's IT systems, user accounts or hardware. All authorised users, including staff, contractors, consultants, and Board members require access to and will use IT systems, hardware, and user accounts to fulfil their roles for and on behalf of the Association.

Definitions	• **IT systems**: all electronic data processing, information, recordkeeping, communications, telecommunications, account management, inventory management and other computer systems (including all computer programs, software, databases, firmware, hardware, and related documentation) and Internet websites.
	• **IT user accounts**: user accounts connect a user to an information service, software application and/or computer network. User accounts determine whether a user can connect to a computer or network and the level of authorised access.
	• **IT hardware**: any PC, laptop, tablet, mobile phone, or other computing device or communication technology issued by Maryhill Housing.
	• **Authorised user(s)**: anyone authorised to access any IT systems, hardware or accounts covering staff, temp workers, consultants, Board members and occasionally contractors, vendors or suppliers.
	• **IT administrator**: a user with administrative level access, whether permanently or on a per-incident or standby basis (IT team)
	• **Maryhill Housing**: Maryhill Housing Association and all its subsidiaries including Maryhill Living.
	• **Association**: Maryhill Housing Association and its subsidiaries
	• **Inappropriate content**: refers to any content that is unreasonable within a professional business environment. This includes but is not limited to:
	  ○ pornography, indecency, or obscenity.
	  ○ information encouraging criminal skills or terrorism, materials relating to cults, gambling, or illegal drugs.
	  ○ any text, images or other media that could reasonably offend someone; based on race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other protected characteristic.

	○ materials that might be considered, in that context as a personal attack, or might be considered as harassment. ○ material that might be defamatory or incur liability or reputational damage for the organisation.
Approval	Senior Management Team – December 2023
Policy Owner	Siobhan Harvey, Business Transformation and IT Manager
Review	Business Transformation and IT Manager – October 2024

Contents

1 Acceptable Usage

Use of Maryhill Housing IT systems, hardware and user accounts, is necessary to support delivery of services and good governance to achieve the goals and objectives of the Association. Maryhill Housing has a policy for the use of IT systems, user accounts and hardware, whereby authorised users must ensure that they:

- comply with current legislation.

- use the IT systems, user accounts and hardware in an acceptable way
- do not create unnecessary business risk to the association through their misuse

1.1 Unacceptable Use and Behaviour

The following is deemed unacceptable use or behaviour by any authorised user:

- viewing, downloading, creating, or distributing any inappropriate content
- viewing, downloading, creating, or distributing any Maryhill Housing information through an unauthorised IT system, user account or hardware. For example, using a personal email account to communicate with customers, using an unsanctioned cloud storage service to store/share data and information or connecting personal storage devices to the organisation network.
- using any IT systems for illegal or criminal activities including fraud, hacking/use of malware, piracy, or copyright infringement.
- any “hacking”, “jailbreaking” or “rooting” without explicit business need and authorisation from an IT administrator.
- publishing defamatory and/or knowingly false material about Maryhill Housing, your colleagues and/or customers, on social networking sites, blogs, wikis, or any other online publishing format.
- revealing confidential information about Maryhill Housing in personal online posting.
- unauthorised upload or transmission - including financial information and information relating to our customers, business plans, policies, staff and/or internal discussions.
- broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters from Mayhill Housing user accounts or hardware.
- transmitting unsolicited commercial or advertising material.
- use of association IT systems, user accounts or hardware for non-business purposes except where explicitly allowed by this policy.
- using an IT system, user account or hardware to breach any other Maryhill Housing Policy, for instance by contravening the Privacy Policy in the sending of confidential information externally.

1.2 Intellectual Property Ownership

If you produce, collect and/or process business-related information in the course of your work, the information remains the property of Maryhill Housing. This includes information stored on third-party websites such as webmail service providers and social networking sites, for example Facebook, LinkedIn, X (Twitter)

1.3 Personal Internet Use

The association recognises that the internet is embedded in many people’s daily lives. As such, it allows authorised users to use the internet for personal reasons, with the following stipulations:

- IT authorised user accounts, specifically email addresses, should NOT be used for any personal subscription services or apps.
- Personal internet use should be of a reasonable level and restricted to non-work times, such as breaks and lunchtimes.
- Inappropriate content is always inappropriate, no matter whether it is being accessed for personal or business reasons using Maryhill Housing authorised user accounts and devices.

2 IT Hardware

These rules minimise the Association's exposure to information security risk as well as increase the user's personal safety and safeguard the Association's IT hardware.

2.1 General Responsibilities - Authorised Users

- IT hardware is the property of Maryhill Housing. It is not acceptable to allow anyone else to use or access it.
- When leaving your device switched on but unattended, in any location, you must activate the password protected lock screen or turn it off.
- IT hardware is the property of Maryhill Housing, and as such must not be altered without permission from an IT administrator.
- When working remotely with your IT hardware, always keep it secured and within sight. If you travel with IT hardware in your vehicle, ensure it is hidden from view and your vehicle is locked when unattended.
- IT hardware should not be taken or used outside the UK. In the rare event that this is required for specific business reasons, you must advise the IT department in writing.
- User accounts created for use on a Maryhill Housing device, must be created using the format @maryhill.org.uk. If you require an Apple ID or Google Account, arrange this with IT so they retain the ability to recover the device when it is returned or requires maintenance.
- Do not remove protective covers, cases, screen protectors etc. from the device. If there is a problem with any protective accessory, contact IT.

2.2 General Responsibilities - Leavers

- IT hardware should be returned on the last day of employment or if the staff member is on annual or sick leave then arrangements should be made to return the equipment within 5 working days of the last day of employment.
- IT hardware must be returned to IT, HR, or the relevant line manager.
- If a PIN is used for security, this user must be changed to the association standard PIN when returning the device. If you don’t know how to change it, you must advise IT of your PIN so they can access the device for wiping.
- When Board membership ceases, Board members should arrange to return any Maryhill Housing devices to the Performance and Governance Manager.
- If IT hardware is damaged, lost or stolen in your care, you must report this immediately and advise of the circumstances and reason for the loss or damage. We appreciate that genuine accidents can happen, and only if negligence is a significant factor, could you be liable for costs associated with the incident.
- If hardware is not returned at least seven days before your final salary payment date, Maryhill Housing reserve the right to deduct estimated replacement costs from your final salary.

2.3 Remote Working

Remote working covers working from home or any other location that is not your normal place of work.

- IT hardware should be stored inside your home, somewhere it cannot be easily seen from outside. Do not leave IT hardware in your vehicle overnight.
- When not in use, keep devices in a safe place, out of reach of children and pets.
- Do not allow any use that is not authorised by Maryhill Housing.
- Do not be tempted to use near water or other liquids that could damage the device.

- Avoid using public and open wi-fi networks wherever possible, for example coffee shops or fast food outlets. Try to:
    - Use named / preferred networks in hotels or other organisations.
    - Use your encrypted domestic WiFi
    - Use your Maryhill Housing mobile phone as a mobile hotspot.

All users should complete a home DSE assessment, before working from home, to ensure they have a safe working environment away from the office.

2.4 Liability

Authorised users are responsible for devices in their care. They will be asked to sign a document during the IT induction process which will be held by HR.

They must report damage or loss immediately to the IT Service Desk servicedesk.maryhill.org.uk and their Line Manager. This allows IT to disable lost or stolen devices and user accounts, where possible, to minimise risk to the Association. An email can be sent to IT, IT@maryhill.org.uk or ask a colleague to raise a ticket via the service desk.

Failure to report damage or loss may result in the authorised user being liable for costs (e.g. mobile phone call costs if not reported lost)

If damage is caused through negligence (including allowing others to use device), the authorised user may be held liable for replacement costs to a proportionate level to be agreed on a case by case basis. Repeated incidents may result in disciplinary proceedings.

Board members should inform the Performance & Governance Manager of any damage, loss, or theft of IT hardware.

3 Security

3.1 Password Policy

1. All user accounts provided for association resources are for individual use and sharing any password with anyone else (including Maryhill Housing managers or IT) is prohibited.
2. All passwords must comply with Maryhill Housing's password policy:
    a. Must be at least twelve characters in length (see guidance below)
    b. Must not be re-used across different systems, neither at home or at Maryhill Housing
    c. Must not reuse / recycle passwords (restrictions have been set)
3. If you have any suspicion that your password has been compromised, you must immediately change it and inform the IT Service Desk.
4. IT may receive 'User at Risk' reports from Microsoft. IT reserves the right to change your password where they assess that a user has been compromised. The user will be contacted in these circumstances and asked to change the password on their next login or when deemed safe to do so.
5. Muli-Factor Authentication (MFA) will be applied to all Microsoft user accounts as standard.

3.2 Password Guidance

Following guidance from the National Cyber Security Centre and in accordance with the Cyber Essentials security standard, Maryhill Housing have adopted the #thinkrandom approach to passwords.

To ensure you have a strong password, consider using three random words (you can include special characters and numbers), for example, *horse1-battery-staple!* Due to the length of the password, it is more cryptographically secure and harder for criminals or hacking software to crack.

3.3 Physical and digital access control

Physical and digital access to Maryhill Housing IT systems, user accounts and hardware is granted by IT on behalf of the Association. Activity across all systems will be monitored both manually and with automated software.

Security alerts will be investigated by the IT team and access may be removed or suspended if there is any compromise of the Associations systems or security. IT reserve the right to disable user accounts and / or change passwords if there is a risk to the Association's data or security.

3.4 Cyber Awareness Training

Once a year, all Staff and Board members must undertake Cyber Awareness Training, delivered via iHasco. It is your responsibility to ensure you complete the training. Failure to do so may result in a user's account being disabled until the course is completed.

3.5 Unannounced Testing

The IT Department may, without warning, run simulated tests for Cyber Security and Disaster Recovery (DR) purposes. Security tests may include, but are not limited to:

- Simulated phishing campaign - sending emails all staff and Board members to see if they will action the email. These phishing tests allow us to gain a valuable insight into the awareness of users.
- System failure – deliberate disconnection of the network to simulate disaster recovery scenarios.
- Penetration Test - attempts to externally hack our networks to test security

3.6 Reporting Breach of Policy

Where this policy refers to reporting, for instance, loss or damage, or security concerns, this means that you must inform your line manager and IT. Board members should inform the Performance & Governance Manager of any issues with their IT equipment. Staff should raise a Service Desk ticket where possible via https://servicedesk.maryhill.org.uk/ Alternatively an email can be sent to IT central mailbox IT@maryhill.org.uk

4 Use of Other Devices & Access

The Association's policy is that only devices provided by and managed by the Association should connect to any Association network or access any Association data.

Personal devices should not connect to the Association's network(s), access Maryhill Housing's data, download or save data to that device or otherwise be used for work purposes.

In exceptional circumstances, you may be permitted to use a personal device with express agreement from IT. It will be your responsibility to ensure that you have adequate cyber security provision on your device including strong passwords and up to date anti-virus software.

4.1 Guidance

This section serves to outline the Association's policy on the use of non-corporate devices for work purposes. It is intended to minimise the Association's exposure to information security risk and promote compliance with data protection regulations.

For this section a “device” is a personally owned laptop, tablet, mobile phone, or other computing device capable of connecting to a network or otherwise accessing association data.

For this policy “reasonable steps” to secure a device are the steps that would reasonably be expected of any professional working with IT equipment and include:

- Those set out in this IT Acceptable Use Policy.
- Being aware of the environment and that you are not being overseen.
- Not connecting to unknown networks without verifying through signage or staff, e.g., of a hotel or café.
- Logging out after each session.
- Reporting any suspicious activity.

4.2 Exemptions

There are a small number of specific exemptions to this policy that relate to accessing online accounts.

Microsoft 365 Online

Maryhill Housing Microsoft 365 user accounts allow access to M365 online.

https://www.office.com

Any authorised user with a Microsoft account can access applications such as Word, Excel, Outlook, and Teams online using the link above. However, please note they will need to verify their login using their preferred multi factor authentication method.

Multi factor authentication will have been set up during the IT induction. You will have confirmed your preference to receive a code or authorisation request via:

- Text message
- Microsoft Authenticator App
- Email

It is recognised that from time to time, staff may wish to access their association email or other Microsoft 365 (M365) applications from non-corporate devices. M365 online is designed and secured to enable access from anywhere, and this risk is judged to be acceptable.

However, access to M365 online does not allow access to Maryhill Housing’s shared drives. These should only be accessed using an authorised device via the Maryhill Housing VPN.

It is not acceptable to download or store any association data or documents on personal devices.

TeamViewer

TeamViewer is a remote access support tool primarily used by IT to assist users remotely. It is designed to be securely accessed from anywhere. It has been risk assessed as acceptable.

4.3 WiFi Networks

It is not acceptable to connect any non-authorised devices to Maryhill Housing's local area network (LAN), or the association's WiFi networks as these permit access to Association data. This will be monitored and IT reserve the right to block and disconnect any unauthorised devices / connections.

Personal devices can be connected to the Maryhill Housing's Guest WiFi network, where it is available and required. Guest WiFi access can be shared for example, where contractors/vendors are presenting or working in our offices, or where staff connect personal mobile phones to the Guest WiFi for internet use during breaks etc.

This is a privilege extended to all authorised users and is provided on the basis that it will not be abused. Use of WiFi access for purposes that would violate other association policies or laws, or impact access or performance for other users, will result in this privilege being revoked.

5 Software Procurement, Installation and Maintenance

5.1 Procurement

IT hardware or software needs to be procured in line with Maryhill Housing policies and budgets. Any request for new hardware or software must be raised with IT who will assess the suitability, compatibility, and cost effectiveness prior to purchase.

5.2 Using and Installing Software

The IT department provide Authorised users with the software they need to do their job role. Any difficulty with software or access should be reported to the IT Service Desk.

Commercially licensed software is the property of Maryhill Housing and may not be copied or distributed from Maryhill Housing owned systems by any users for any purpose.

Only IT administrators are permitted to install software, including patches or modules for existing installed software which may alter, increase, or decrease functionality.

Maryhill Housing mobile devices are enrolled with mobile device management software (TinyMDM or InTune) that allows IT to track and disable devices where security is compromised. Pre-approved Apps are accessible to users via the associations Play Store. If there is a specific business need for new or additional apps, users should submit a request to IT Service Desk.

5.3 Approved Software

Only approved software should be used by staff. IT may use additional approved software and applications that include additional software for testing, diagnostics, and evaluation purposes to allow them to fully support the association and its users.

The approved software list is maintained by IT.

5.4 Maintenance

Core equipment (servers, switches, firewalls, ONTs and other cabling/equipment in each office's rack/server room) must not be accessed or changed by anyone other than an IT administrator.

IT may temporarily designate someone an IT administrator to assist with remote troubleshooting to assist with resolution of an incident or issue.

In the event of any visits from contractors, suppliers, vendors etc. who need to have access to IT systems for a business need, this must be authorised by IT in advance and will be carefully controlled on the principle of least privilege.

5.5 Use of WhatsApp

Any communication with tenants or external contacts on behalf of the Association should be carried out using a secured Maryhill Housing mobile and user account. Tenants may need to use WhatsApp to communicate where they have no phone credit but wi-fi access.

The WhatsApp platform encourages less formal communication but please be aware that your interactions may be reviewed against any complaints and so be mindful that you are still presenting the Association and maintain a level of professionalism at all times in line with our values.

Occasionally, with prior agreement from the participants, WhatsApp groups may be set up using personal device details. The main example being for Disaster Recovery purposes where out of hours alternative contact is necessary.

5.6 IT Support

IT support requests must be submitted to servicedesk.maryhill.org.uk. A Service Desk user guide can be found here.

Board members should inform the Performance & Governance Manager of any issues with their IT equipment, the Performance & Governance Manager will liaise with IT Support.

6 Policy enforcement

Users should always ensure that data transmitted through or stored on any Maryhill Housing IT systems is accurate, appropriate, ethical, legal and complies with GDPR guidance.

All data transmitted through IT systems is part of official Maryhill Housing records. The Association can be legally required to show that information to law enforcement agencies or other parties such as the Information Commissioners Office (ICO) or for a Subject Access Request (SAR) or Freedom of Information request (FOI).

6.1 Potential Sanctions

Knowingly breaching the Acceptable Use Policy can have serious consequences. Staff who do so may be subject to disciplinary action, up to and including termination of contract. Board members actions may be investigated in line with the breaches of Code of Conduct process.

In serious circumstances, authorised users may also be held personally liable for violating this policy as certain elements reflect criminal law. Where appropriate, the Association will involve the police or other law enforcement agencies in relation to breaches of this policy.

6.2 Monitoring

IT systems, hardware and user accounts are provided for legitimate business use only. The Association therefore reserves the right to monitor and review the information stored or transmitted through those systems, hardware, and user accounts. Any such examinations or monitoring will only be carried out by authorised IT administrators in accordance with our Privacy Policy.