| | |
|---|---|
| **Title** | **ICT Acceptable Use Policy** |
| **Purpose** | The purpose of this policy is to provide a framework within which users will work when accessing ICT systems and the data they contain whilst ensuring the safety and security of the ICT network, infrastructure, systems and data which the organisation uses. |
| **Scope** | This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy may exist: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points; for example: the Visitors Code of Conduct.<br>This policy covers the use of Maryhill Housing's systems whether they are accessed on-premises or remotely. |
| **Definitions** | "**Users**" are everyone who has access to any of Maryhill Housing's ICT systems. This includes all employees and others working on behalf of the organisation.<br>"**Systems**" means all ICT equipment that connects to the corporate network or access to corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.<br>"**ICT**" means Information & Communications Technology. This term covers all technology as it relates to the storage, retrieval, transmission, archival and processing of information or data in an electronic form.<br>"**AUP**" means Acceptable Use Policy as it relates to the use of the organisation's ICT facilities.<br>"**Hardware**" means physical computer equipment, including workstations, monitor screens, Keyboards, Mice, Tablets, Laptops etc.<br>"**Software**" means Computer software (often called just software) and is made of one or more computer programs. Sometimes it means one specific program, or it can mean all the software on a computer, including the applications and the operating system. Applications are programs that do a specific thing, such as a game or a word |

| | |
|---|---|
| | processor. The operating system (Mac OS, Microsoft Windows, Linux, etc.) is software that helps the applications run, and controls the display, the keyboard and mouse.<br>“**CCTV”** means (closed-circuit television ) a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.<br>“**MH”** The term as it is applied throughout the policy means Maryhill Housing. |
| **Policy Statement** | This Acceptable Use Policy (AUP) designed to protect Maryhill Housing, our board members, employees, customers and other partners from harm caused by the misuse of our ICT systems and our data. Misuse includes both deliberate and inadvertent actions.<br>The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), our reputation, legal and financial penalties for data leakage and lost productivity resulting from network downtime.<br>Everyone who works at Maryhill Housing is responsible for the security of our ICT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their Line Manager or the ICT Manager.<br>**Use of ICT Systems**<br>**General**<br>Maryhill Housing’s ICT systems exist to support and enable the business and are intended primarily to support our strategic objectives as described in the Corporate Plan.<br>Users may not use the organisation’s ICT facilities to carry out activities which constitute either commercial activity, (except as authorised, in the exercise of their duties as it relates to organisation’s business), or for personal profit or gain.<br>Only approved and authorised hardware such as computer workstations, laptops, tablets and mobiles, including smart phones, may be used to access the corporate network and its resources. Staff are not permitted to connect their own personal equipment to the network without prior approval, this includes items like your own laptop, USB or adding a Wireless Access Point for Wi-Fi provision.<br>**Remote Access**<br>The organisation operates a Microsoft Windows Remote Desktop Server for the purpose of remote working from out with the corporate network. Users connecting to the systems from any of the |

organisation’s other offices will be connected securely over either a dedicated wide area network link (in the case of the Glenavon Neighbourhood and Glenavon Sub-Office) or a Virtual Private Network (VPN) connection.

Access to the systems from other locations for example, a user’s home, is not permitted unless specifically authorised in line with the Home Working Policy.  These include Tablet computers issued to board members and tablet computers provided to staff for use when they are out of the office.

Users working from home must adhere to the Working from Home Policy and observe the Health and Safety checklist provided in the appendix of that policy.

### Mobile Phones/Devices

All of the equipment are the property of the organisation and not the property of one individual.  All phones, chargers etc should be made available for use by other members of staff as and when required. It should be remembered that one of the main reasons for having them is to deal with organisation business and emergency situations only. The use of phones is mandatory for when working out of the office for health and safety and lone working and staff should be contactable when working out of the office.

All mobile phones and devices will be recorded centrally on the ICT Asset Register by make, model, serial number, IMEI number and what member of staff the equipment has been allocated to.

All members of staff allocated a mobile phone or device have a duty of care to look after the device and are responsible for returning the device on leaving the organisation.

### Personal Use

A small amount of personal use is, in most cases, allowed. However, personal use must not be in any way detrimental to users’ own or their colleague’s productivity.  Neither should it result in any direct costs being borne by Maryhill Housing other than for trivial amounts (e.g., an occasional short telephone call, or the printing of a few pages). Under no circumstances should staff or board members allow unauthorised personnel access to the organisation’s equipment at any time or for any purpose.

Maryhill Housing trusts users to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s ICT systems. If employees are uncertain, they should consult their manager in the first instance or the ICT Manager.

### Monitoring and Auditing

Please refer to the separate Employee Monitoring Policy which sets out how Maryhill will monitor employees and their use of ICT systems.

### Data Security

### Access to Systems and Data

Users are accountable for using the ICT facilities in a responsible, ethical and lawful manner and may only access the systems to which they have been authorised to do so.

If data on Maryhill Housing’s systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorised access to confidential information, such as locking their computer screen when away from their desk. Users must also log off and shut down their computer and monitors when they are leaving the office for the day in order that any planned network security patches and updates are applied successfully. Failure to comply with this poses a risk to the security of the data and network which we operate.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential. If in doubt, please ask your manager for guidance.

Users must not send, upload, remove on portable media or otherwise transfer to a non-Maryhill Housing system (e.g. Dropbox or similar) any information or data that is designated as confidential or personal, or that they should reasonably regard as being confidential to Maryhill Housing unless it has been encrypted, and where explicitly authorised to do so in the performance of their regular duties.

### User Account Passwords

All system passwords are confidential and Users must keep passwords secure and not allow others to access their accounts.

Maryhill Housing has a Password policy which requires users to select a new, complex password every 60 calendar days. Passwords are made up from numbers, letters, characters and words.

Users must observe this good practice.

If you require your password to be reset, please contact the ICT Team.

The ICT team should never request that you send them your user password by email.

Do not send requests to have another user’s password reset. This should be requested by your Line Manager, who should also state the reason for authorising. All requests should be sent to the ICT Group mailbox.

### Phone System Voicemail PIN Numbers

PIN Numbers for accessing voicemail should be kept personal and confidential.
They should not be shared with others unless there is a reasonable case for doing so. An example may be when you are on holiday.

If you need to provide another member of staff access to your voicemails you should clear this with your line manager first and follow the guide note below:

- Change your PIN code to a new one
- Inform your line manager or colleague as needed
- Set a new PIN code upon your return to work.

### Use of mobile data on Maryhill devices and public wi-fi

Staff issued with mobile phones with data functionality need to ensure this is used responsibly and cost effectively.

In general you should only be using Maryhill phone data when you are working remotely and no Wi-Fi is available

You should only ever be using your work phone data for work purposes, except in exceptional circumstances.

You should turn off personal hotspots when devices stop being tethered and in use

If you are working from home you are expected to use your home Wi-FI and you should ensure it is password secured and not open to the public.

If you are in the office you should be accessing the secure office wi-fi, not the guest network.

Free Wi-Fi provided by shopping centres, cafes, airports and restaurants are all classed as public. This type of Wi-Fi is not as secure as the Wi-Fi at home or in the Maryhill office. It is worth being aware of the potentials risks such as fake/bogus networks and that there could be malicious attempts to redirect users to fake/bogus websites. It is recommended that web browsing is minimised and that secured apps, such as email are used. If web browsing is required then it’s recommended to type the website address (URL) into the address bar of a web browser rather than relying on search results.

If any strange prompts or requests for access to device/data, or requests for payment are displayed then its best to disconnect from the Wi-Fi network, turn off Wi-Fi on device and use the mobile data connection.

Unless required for work purposes, streaming on the data connection should be avoided.

**Privacy**

Please refer to the Employee Monitoring Policy which sets out the situation whereby Maryhill will access the records of individual employees.

**Responsibilities**

Users who are supplied with computer equipment by Maryhill Housing are responsible for the safety and care of that equipment, and the security of software and data stored on it and on other Maryhill Housing systems that they can access remotely using it.

Equipment issued to board or staff members is subject to their signing of the Declaration of Receipt of Association Equipment.

All users must adhere to the Code of Conduct policies in respect of all electronic communications and data.

**Portable Devices**

Information held on portable devices, such as laptops, tablets and smartphones, is especially vulnerable and special care should be exercised with these devices. Information should not be stored on the device at all. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it. If in doubt, please seek advice from the ICT Manager.

No member of staff should carry with them any USB flash drive containing personal data from MH systems which is unencrypted. Neither should any member of staff save personal data from MH systems to their own hard drive, tablet or mobile phone.

**Workstations**

All workstations (desktops and laptops) and Tablets will be secured with a lock-on-idle policy active after 5 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended for any length of time, however brief.

If it is expected that you will be away from your desk for longer than 60 minutes, you should Log Off from the workstation.

There are clear practical reasons for either Locking or Logging off from the workstation, which include, but are not limited to:

- Power Failure resulting in the loss of un-saved documents
- Exposure of confidential information

**Security Software**

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into Maryhill Housing's systems and must report any actual or suspected malware infection immediately. To not do so may potentially expose the organisation to loss of data or ICT facilities or both.

All workstations are required to have up-to-date Anti-Virus & Anti-Malware protection at all times for the safety and security of Maryhill Housing systems and data.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

**Network Data Storage and Transfer**

Maryhill Housing has a centralised Storage Area on its Network for the storage of all data (Word Documents, Excel Spreadsheets, and PowerPoint Presentations etc.).

All users of the system should store any and all important files/data in these common locations, especially if it is data relating to MH business or files generated in the exercise of daily duties.

Files received as attachments in an email that relate to organisation business should be saved in the appropriate network drive.

Users should not keep any files on their PC's local Hard Disk Drive (the 'C' Drive) or on Removable Media such as USB Memory Sticks as it is NOT backed up and therefore at risk. Storing files or folders on your computers' "Desktop" is not permitted, except on a temporary basis.

If files are transferred temporarily to one of MH's laptops or computers, it is the responsibility of the user to ensure they are deleted when they are finished using them. Confidential files must not be left on any portable computer type, be it a laptop or company smart phone, as this may expose MH to the risk of being in breach of the General Data Protection Regulation.

**Internet Access and Email**

The organisation has Internet Access as part of the overall communications infrastructure. Access to Internet Resources

(Websites and other services) is provided to all users of the systems for the purpose of responding to customers, research, accessing National and Local Government Online Services, Partner Agencies, Companies, digital and social media communication and Suppliers and Email communications etc.

Occasional and reasonable personal use is permitted, provided that this does not interfere with the performance of your duties. In this regard occasional and reasonable personal use is to be limited to:

1. Before you have clocked in to start work
2. During your lunch time break (where you have clocked out)
3. After you have stopped working and have clocked out

The Internet should not be used for personal use at any other time.

Access to Internet Web Sites is controlled by a Website/Content Filtering service at both the Browser on the workstation, using Bitdefender Security Software as well as the perimeter Firewall.

Content filtering restricts access to only those categories of sites which are deemed appropriate in the performance of your duties. Inappropriate websites and content which are attempted to be accessed will be rejected along with a relevant deny message.

### Email Guidelines

The organisation operates an Email Server for its registered Internet Domain Name “maryhill.org.uk” and each staff member is provided with an email account.

Maryhill Housing email accounts are provided for the purposes of official organisation communications and correspondence. A reasonable amount of personal correspondence is deemed acceptable. However staff and board are encouraged to use their personal email accounts for personal correspondence.

Maryhill Housing email addresses are not be used to sign-up or register for on-line services or similar except where there is a genuine business requirement, for example; EVH newsletters or services.

### Email Etiquette

Be aware that correspondence via email is treated as a legal form of communication and as such, when corresponding with external parties, that you are representing the organisation. Avoid the use of personal opinions and if used, it should be clearly indicated that they are such.

Check your inbox at regular intervals or make use of the notification facility within Outlook which indicates new messages have been received.

Always ensure that your emails contain the organisation’s standard Email Signature in the prescribed format. This is detailed in the ICT Policy.

Treat others with respect and in a way you would expect to be treated by others (e.g. do not send unconstructive feedback, conduct an argument or invite (or incite) colleagues to publicise their displeasure at the actions / decisions of a colleague).

Please don’t forward emails warning about viruses, as they are invariably hoaxes and ICT Support will probably already be aware of genuine viruses. If in doubt, ask ICT for advice.

Do not take part in chain emails (chain letters) or forward joke emails. If you receive an email of this nature, you should delete it without delay and do not reply to the sender. Not everybody shares the same sense of humour and you should not forward messages of this nature to multiple recipients or any distribution list. You should remain mindful of what you are sending to ensure you are not breaching the Code of Conduct or Dignity at Work Policies. If in doubt, please refer to these policies for further guidance.

### Email Attachments

Special attention should be paid to email attachments received from outside parties. While we use an external service (Everycloud) to scan all email attachments for viruses and other threats prior to reaching our email system, there is always the possibility something can slip through. If in doubt about an email attachment, do not open it. Seek advice from ICT.

Forwarding attachments around our system unnecessarily needlessly adds to the number of duplicate files held in our systems and should be avoided. Instead please save the attachments to the network drive and inform colleagues where you have saved the file by using a hyper-link to direct others to the location of the stored file.

### Social Media

The organisation recognises that Social Media has a role to play in terms of communication with tenants, resident groups and a wider audience in general. Access to Social Media Platforms is permitted on Association Workstations, Tablets, Laptops and Smartphones. Staff are encouraged to use Maryhill social media profiles to communicate with tenants and other stakeholders.

It is also acceptable to use social media for personal use when not clocked in, for example at lunch.

The organisation also recognises and respects both the employee’s and board members rights to a private life which includes joining any social media platforms they wish. However, information posted on such sites is classed as public and not private. This applies whether you are posting under your own name or a pseudonym.

Board Members and Employees are therefore not allowed to disclose confidential information relating to Maryhill Housing, its customers, partners, suppliers, other board members and employees, or stakeholders on any social networking platforms. It is also prohibited to post any comments on people and events connected to Maryhill Housing, or make any remarks which could potentially bring the organisation into disrepute. Any such actions could result in disciplinary action, including dismissal.

If using social media platforms, board members and employees are expected to adhere to the following:

- Keep profiles set to private and protect tweets if using Twitter
- Ensure all passwords are kept private.
- We do not prohibit employees from listing Maryhill Housing as their employer however we do advise against it.
- Board Members and Employees should be aware of the language and content of their posts – in particular where there is an association with their employer e.g. listing their employer or linked with colleagues.

**Data Protection and General Data Protection Regulations**

Maryhill Housing takes Data Protection seriously and takes all relevant steps and precautions in ensuring compliance with the legislation (Data Protection Act/General Data Protection Regulations).

The introduction of the new General Data Protection Regulation (GDPR) is the biggest change to data protection law in over 20 years. It applied from 25 May 2018.

Personal data is information that concerns living individuals. It includes individuals’ names, contact details and any other information that identifies them from other individuals. Some personal data is regarded as being more sensitive and this includes information about an individual’s: racial or ethnic origin; political opinions; health; sexual life or sexual orientation; religious or other beliefs; or trade union membership status.

The GDPR will apply to all electronic personal data held by MH and paper personal data that is ‘accessible according to specific criteria’. This covers personal data in MH paper files that is structured in a way that it is possible to find the personal data that you are looking for without much difficulty.

A set of MH tenancy files stored in a filing cabinet in alphabetical order (by tenant name or property address) with papers in the file sorted in reverse time order will be covered by the GDPR.

Processing is anything that MH does in relation to personal data, from when it is collected or created to the point that it is deleted or destroyed.

The GDPR is a complex law and below are the 10 key changes from the DPA introduced by the GDPR on 25 May 2018.

1. Collecting personal data
2. Consent to personal data collection and use
3. Accountability framework
4. Keeping MH's personal data secure
5. Engaging with MH's service providers
6. Data retention
7. Data Protection Impact Assessments (DPIA)
8. Appointment of Data Protection Officer (DPO)
9. More rights for individuals
10. Tougher penalties

Data accessed, held or processed by the organisation is subject to the organisation's Data Protection Policy and all employees should take the security and integrity of data seriously.

**Limitation of Liability**

Maryhill Housing accepts no liability for any loss whatsoever, howsoever incurred, by any individual, making use of the Internet Access facilities to make a payment/purchase online and indemnifies Maryhill Housing against any such losses incurred.

This includes;

1. Loss of personal data and or files stored on any workstation, server or mobile device owned by Maryhill Housing – the organisation is under no obligation to perform data recovery of this nature.

2. Loss of monies as the result of Online Fraud or similar. - All users are advised that making purchases online can represent a financial risk and as such it is incumbent upon the individual user to check and verify they are using a legitimate website and payment system, **before** providing payment information and personal details. If in doubt, do not proceed.

   Legitimate websites will have a valid SSL Certificate issued by a Certification Authority to indicate they are using encrypted communications (normally indicated by the presence of a Padlock Symbol on the browser window's address bar).

**Unacceptable Use**

All employees should use their own judgment regarding what is unacceptable use of Maryhill Housing’s systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of Maryhill Housing. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include;
    - activities that slow down the computer network and or Internet Connection (e.g., streaming audio or video, playing online or networked video games, peer-to-peer file sharing or ‘Torrent’ applications).
- All activities that are inappropriate for Maryhill Housing to be associated with and/or are detrimental to the *company’s* reputation, or which are prohibited by the Equality and Diversity & Dignity at Work policies. This includes but is not limited to, pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the ICT security systems and protocols which Maryhill Housing has put in place.
- Excessive or repeated use of the Association’s printing facilities for personal purposes.
- Using a ‘maryhill.org.uk’ email address to register for online services like eBay, PayPal, Amazon, Tesco, Sainsbury’s, M&S, Coupon Vouchers etc unless expressly authorised to do so. Use a personal email account, like Hotmail or Google or Yahoo for this.
- Accessing websites and Internet services that are not in any way connected with Association business during core working hours.

Should an employee need to contravene these guidelines in order to perform their role, they must consult with and obtain approval from their manager before proceeding. Should you inadvertently access a site which is inappropriate, please report immediately to either your manager or the ICT Manager.

**Acceptance of the Policy**

All Users (as previously defined) are expected to sign their acceptance

| | |
|---|---|
| | of the policy prior to being granted access or provided with access credentials.<br>Particular attention should be paid to the policy as it relates to Internet Access and Email use. The Association sets out its approach to monitoring this in its Employee Monitoring Policy.<br>The organisation or its authorised representatives may retrieve the contents of email messages for the purpose of monitoring and/or ensuring quality standards and legitimacy of use. The organisation does not routinely or proactively monitor Internet or email communications, but does however retain logs relating to Internet access and email for the purpose of statistical analysis, fault diagnosis and auditing.<br>**Breaches and Enforcement**<br>Maryhill Housing will not tolerate any misuse of its systems. Anyone found to have deliberately contravened this policy, including not exercising reasonable judgment regarding acceptable use will be subject to the organisation's Disciplinary Procedures. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.<br>The use of any of Maryhill Housing resources for any illegal activity will normally be grounds for summary dismissal and Maryhill Housing will not hesitate to cooperate with any criminal investigation and prosecution that may result from such activity.<br>The following are some examples of breaches of this policy and this list is not exhaustive:<br>• Concealment or misrepresentation of names or affiliations in e-mail messages.<br>• Alteration of source or destination addresses of e-mail.<br>• Use of communication tools for commercial or private business purposes.<br>• Use of communication tools, in a way that unreasonably interferes with or threatens other individuals.<br>• Use of communication tools that degrades or demeans other individuals – whether Maryhill Housing employees, board members or any other individual.<br>• Any form of commercial use using communication tools is prohibited.<br>• Use of Internet Access for personal reasons during working hours where you have clocked in for work. |
| **Approval** | Staffing Committee, 10 September 2018 |

| | |
|---|---|
| **Policy Owner** | Bryony Willett<br>Chief Executive |
| **Review** | Maryhill Housing will review this policy every three years and monitor the effectiveness of this policy to ensure it continues to meet its aims and objectives. |