Community Counts

Milnbank

Housing Association

53 Ballindalloch Drive, Glasgow G31 3DQ

IT & ACCEPTABLE USE POLICY

JH/PH/JULY2020/REF.P30

☎ 0141 551 8131 0141 550 2060 admin@milnbank.org.uk www.milnbank.org.uk

A registered Scottish Charity No.SC039891 Registered: Scottish Housing Regulator.
Registration No. HCB 161 SC Registered: Financial Conduct Authority - 1818 R(S).
Registered under the Co-operative and Community Benefit Societies Act 2014.

1. AIM OF POLICY

The aim of the IT & Acceptable Use Policy is to clarify the principles that govern the use of the IT and related facilities provided by Milnbank Housing Association (MHA). The policy details MHA's position on how its users communicate internally and externally, whether for business or personal use.

All employees who use the Association's electronic facilities have access to policies on an on-going basis. New employees, at the commencement of their employment, are issued with a list of the policies within the Condition of Service and are advised to read these.

2. GENERAL DATA PROTECTION REGULATIONS (GDPR)

GDPR regulations came into force on 25 May 2018 and they placed a greater responsibility on all organisations to ensure that the personal data the Association holds is secure, accurate and up to date.

MHA control the personal information that we collect, this means that we are legally responsible for how we collect, hold and use your personal information. It also means that we are required to comply with the General Data Protection Regulations (GDPR) when collecting, holding and using personal information.

This Policy has been compiled to comply with the General Data Protection Regulations (GDPR). Further information can be found in our Privacy Policy.

3. INTRODUCTION

a) IT Hardware

Workstation - To assist effective and efficient business activity, all MHA employees will be provided with access to a reliable and up to date workstation. All workstations have a limited expected useful life and a review will take place by the IT Co-ordinator at the end of the initial three year period and thereafter on an annual basis to ascertain whether replacement or upgrading is required.

Laptops/Tablets - The Management Team, Management Committee and any other relevant staff member will be provided with a company laptop or tablet to enable them to work in various locations. A review to replace laptops will be undertaken by the IT Co-ordinator as noted above. All other employees are permitted to borrow a company laptop for office use in accordance with the IT & Acceptable Use Policy. This information will be recorded in the IT Register.

Servers – All the Association's data is stored on the servers, therefore this item is critical to the provision of an effective network. A back-up of the server is carried out off-site by the Associations IT provider.

b) IT Software

The Association uses Microsoft Office 2013 for office use and Kypera package for integrated modules for all areas of activity. All IT Software will be reviewed annually to ensure it meets the needs of all users.

A register of all IT equipment issued to employees and management committee members will be maintained by IT Co-ordinator.

The IT Co-ordinator will carry out an annual assessment of all IT hardware as part of the budget setting process.

c) IT Support

Reporting Procedures – All problems relating to the computer system should be reported to the IT Co-ordinator to investigate and attempt to solve the problem. However, if external help is required, a call will be logged with MHA's IT Consultant or Kypera Helpdesk and the employee notified of an expected completion time.

Service Level Agreement – is in place to cover hardware support with M2 and is reviewed as and when required to ensure it remains fit for purpose.

4. GOVERNANCE OF IT

a) IT Policy - The Data Protection Officer, with support from the IT Co-ordinator, is responsible for reviewing, implementing, and monitoring the Association's IT & Acceptable Use Policy. The policy will be reviewed on an annual basis or as when required and distributed to all users.

b) IT Procedure Manual - A detailed IT Procedure Manual is available for reference for all MHA employees. This document will be reviewed and updated on an annual basis by the IT Co-ordinator.

c) Risk Management - As a requirement of the organisation, the Corporate Services Manager & IT Co-ordinator are responsible for regularly assessing and updating the Management Team with the risks associated with managing IT. A formal review of the Risk Audit will also be carried out on an annual basis.

d) Associated MHA Policies – IT forms part of the undernoted MHA policies:

- Training & Development - A review of all IT training requirements will be carried out as part of the annual Training Needs Assessment and implemented into the organisational annual Training Plan.

- Health & Safety – All computer equipment requires to be used in line with MHAs Health & Safety Policy.

- Data Protection & Disclosure of Information – The Association's Data Protection and Disclosure of Information Policies should be read in conjunction with the IT & Acceptable Use Policy.

e) IT Security

Full details of MHA's IT security are within the Association's Password Protection Policy.

- Storing Information - All information stored on the main computer server is backed-up each day. All staff have a duty to ensure that any information which they are responsible for is adequately stored in the F: Drive.

- Removable Storage Devices - MHA do not encourage the use of removable storage devices and all staff members should use internal network tools to move corporate data. Using portable data brings the threat of data leakage, data theft, and the introduction of viruses or other malware into MHA computing systems.

- Scanning – A scanning system, whereby all files, correspondence etc., are filed in a corporate format, operates within the Association.

- Removing Data - Staff will be permitted to remove documents and records from the office on the condition that authorisation has been granted from the relevant line manager and that details are logged onto the Removal of Data Form; this can be located in the Standard Forms file (Form 17 Removal of Data).

5. USE OF IT FACILITIES

The use of IT has developed rapidly over the past years and forms a large element of most employees' job. This section of the policy aims to provide guidance on MHAs position in relation to internal and external communication via various modes of IT.

a) Email & Internet Usage

Email is a business communication tool and as such should reflect a professional business image at all times; this applies to emails sent internally within and externally of MHA.

All employees have access to email and internet for use in connection with MHA's business and as part of the normal execution of the job duties. The purpose of these rules is to protect MHA's legal interests. Employees must use the Association's MHA email account. The use of any other email account is strictly prohibited (e.g. gmail, aol).

Employees are permitted to use MHAs email and internet, however, this personal use must be at a reasonable level and this use should only be during personal time (e.g. lunch break). Internet "surfing" is not permitted (E.g. chat rooms, eBay, gambling sites). The parameters for use of the above are:

1) Keeping personal messages to a minimum.
2) Prohibiting use of email for entering into contractual commitments, financial, commercial or private business use.
3) Staff should avoid sending large emails or attachments.
4) Avoid unnecessary copying of emails.
5) Avoid using email for confidential messages.
6) Avoid participating in pyramid letters or anonymous emailing services.
7) Staff should ensure that messages are not trivial, offensive, abusive, defamatory, obscene, discriminatory or harassing.
8) Prohibit access of inappropriate and illegal material, including pornography.

Employees who are discovered contravening these rules, whether inside or outside the Association, may face serious disciplinary action under MHA's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's dismissal.

b) Social Networking

When logging onto and using social networking and video sharing websites and blogs at any time, including personal use outside the workplace, employees must not:

1) Publicly identify themselves as working for MHA, make reference to the Association or provide information from which others can ascertain the name of the Association.
2) Conduct themselves in a way that is detrimental to the Association or brings MHA into disrepute.
3) Use their work email address when registering on such sites.
4) Allow their interaction on these websites or blogs to damage working relationships between employees and clients of MHA.
5) Include personal information about MHA's employees, management committee, residents, contractors or customers without their express consent(an employee may still be liable even if the employee, management committee, resident, contractor or customer are not expressly named in the websites or blogs as long as MHA reasonably believes they are identifiable).
6) Make a derogatory, offensive, discriminatory or defamatory comment about the Association, its employees, management committee, residents, contractors or customers (an employee may still be liable even if the employee, management committee, resident, contractor or customer are not expressly named in the websites or blogs as long as the Association reasonably believes they are identifiable).
7) Make any comments about MHA's employees that could constitute unlawful discrimination, harassment or bullying.
8) Disclose any confidential information belonging to MHA, its employees, management committee, residents, contractors and customers.

A reference to the above is outlined within MHA Employee Code of Conduct which sets out the standards of conduct required of you as a member of staff in relation to social media.

Employees who are discovered contravening these rules, whether inside or outside the Association, may face serious disciplinary action under MHA's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's dismissal.

c) Use of Telephones & Mobiles

Employees are expected to use the telephone for the duties they are employed to undertake. However, MHA recognises that sometimes it is necessary and reasonable for employees to use the office telephone for personal calls. Employees are therefore allowed to make and receive personal calls, as long as they are necessary, reasonable and small in number. Employees are expected to be responsible in exercising this privilege. Personal calls should be restricted to personal time as far as possible, and must not interfere with your work, or the work of others.

MHA permits employees to use mobile phones during office hours for personal use, as long as they are necessary, reasonable and small in number. Employees are expected to be responsible in exercising this privilege. Personal calls should be restricted to personal time as far as possible, and they must not interfere with your work, or the work of others. Text messaging from office mobiles is prohibited unless for business purposes. MHA periodically monitors company mobile phone bills to check data usage.

All employees who are issued with the Conditions of Use Agreement: Company Mobile Phone Statement.

d) Remote Access

Remote access is restricted to line managers, however, occasionally other employees work from home (e.g. using a laptop) or out of the office (e.g. using a iPad/iPhone during a house visit) and the Association stresses that all aspects of the IT & Acceptable Use Policy should be adhered to when working remotely. Employees who are absent from work through sickness should not access Association IT equipment remotely unless authorised by a member of the Management Team.

Management Committee Members who are issued with company iPads must sign and comply with the conditions within the Provision of iPads for Committee Members which forms part of the Governance Protocols.

Remote access will be restricted to the hours of 7am – 7pm with the following exceptions:

- Management Team
- Management Committee
- Support Staff
- Any staff who have been given authorisation for additional access

If remote access is required out-with the hours of 7am to 7pm the form at Appendix 1 should be used to get authorisation from your Line Manager.

e) Computer Software, Games & Viruses

As the Association's computer network is vulnerable to viruses, only duly authorised personnel have the authority to load new software onto the network system and will only do so after having checked for viruses. Any employee found to be contravening this may be subject to a disciplinary investigation.

f) Company Website

MHA has developed a Website as a communication tool for residents and other customers. Access to record changes to the Website is restricted to authorised personnel e.g. IT Co-ordinator, DP Officer & CS Manager. The updating of the website is monitored on a weekly and as required basis.

g) CCTV Cameras

Full details of MHA's CCTV Cameras are within the Association's CCTV Policy.

6. IT MONITORING

The Association will not routinely monitor the contents of the various IT equipment, however MHA does reserve the right to monitor all systems and to inspect at any time, as long as there's a valid business purpose for doing so. This includes:

- Checking emails to ensure the system is not abused
- Recording of telephone calls
- Viewing the office CCTV tapes
- Tracking company mobiles
- Tracking the use of company vehicles.

The Association ensures that employees are aware that monitoring may take place and of the standards they are expected to achieve by distributing updated IT Policy to all Staff.

The purpose of monitoring is to assist in establishing facts which may need to be known for a specific purpose, investigating any suspected or alleged criminal activity, ensure that the Association's systems work effectively and to determine any suspected or alleged abuse of this policy.

Employees who breach this policy will be subject to a disciplinary investigation. If necessary, information gathered in connection with the investigation may be handed to the police. Any employee who receives inappropriate email, or is aware of inappropriate use of the IT system, should report it to the IT Co-ordinator/DP Officer or CS Manager for further investigation.

7. BREACHES OF POLICY

Any breach of the policy, either deliberate or inadvertent, will be subject to investigation in accordance with MHA's disciplinary procedures that may ultimately result in action up to and including dismissal without notice. If any employee feels that acceptable use of any of the IT facilities is being unfairly denied, they have the right to raise this matter in accordance with the Association’s grievance procedure.

APPENDIX 1

REMOTE ACCESS REQUEST

1) Please state reason for requesting remote access?

....

....

....

2) Duration you require remote access:

From (date)............. Effective up to (date)......................

Will you need access outside 7am to 7pm Yes / No

STATEMENT

Employees are reminded that the Association's IT & Acceptable Use and Data Protection Policies remain applicable when using MHA systems outside the office.

Name..

Signed.. Date........................

NOTE 9

Request authorised by: .... Line Manager

Access allowed: .... IT Co-ordinator

Laptop Used: ………………………………….