Community Counts
Milnbank
Housing Association
53 Ballindalloch Drive, Glasgow G31 3DQ

TO:	MHA Board
PREPARED BY:	Pauline Munro, Executive Office
SUBJECT:	IT & Acceptable Use Policy
DATE OF MEETING:	10 March 2026
APPROVED BY:	Paul Martin (CEO)
Version Number:	1
Date of Latest Version:	10 March 2026

IT & ACCEPTABLE USE POLICY

HAPPY TO TRANSLATE

If you have difficulty with reading this policy, including any difficulties with sight or hearing, or if you require this document translated into another language, please contact us and we will be happy to provide this information in a format that suits your needs.

PM/FEBRUARY.2026/REF P30

IT & ACCEPTABLE USE POLICY

CONTENTS

1. MHA's Strategic Objectives
2. MHA's Values
3. Regulatory & Legislative Compliance
4. Policy Introduction
5. Principles of the IT & Acceptable Use Policy
6. Scope
7. Definitions
8. General Responsibilities
9. Communication Standards
10. Information Security Requirements
    - 10.1 Passwords & Access
    - 10.2 Device Protection
11. Report Immediately
12. Personal Use
13. File Sharing & Storage
14. Mobile Phone
15. Non Compliance
16. Equality & Human Rights
17. Data Collection
18. Monitoring & Review of Policy

1. MILNBANK HOUSING ASSOCIATION STRATEGIC OBJECTIVES

MHA's mission is to provide excellent homes and services in a thriving community. We believe that people living in the MHA community should:

- Have warm, safe, and affordable homes, and receive excellent services from MHA.
- Live in neighbourhoods that are clean and well cared for, with real community pride.
- Have access to opportunities and services that promote a good quality of life.

2. MHA VALUES

Working as 'One Milnbank' so that we offer the same quality of services, support and housing to all tenants and residents.

3. REGULATORY & LEGISLATIVE COMPLIANCE

The Management Committee leads and directs MHA to ensure good outcomes for its tenants and other service users. The Scottish Housing Regulator's Regulatory Framework Financial & Regulatory, Standard 2 Tenant & Service User Interests, Standard 3 Risk Management and Internal Controls and Standard 4 Financial Management and Charter Outcomes 2 Communication, Outcome 3 Participation and Outcome 11 Tenancy Sustainment.

4. POLICY INTRODUCTION

This policy defines how MHA systems and communication tools must be used to protect people, reputation, data, and organisational operations.

MHA aims to provide excellent homes and services in a thriving community. Secure and lawful IT use is essential to delivering safe, reliable services.

This policy sets out how MHA IT systems, devices, and communication tools must be used to support secure, professional, and lawful working. It ensures the protection of MHA's people, reputation, data, and technology assets.

MHA adheres to all relevant legal employment requirements associated with this policy. This policy aligns with UK GDPR, Data Protection Act 2018, cyber-security standards, and regulatory expectations.

5. PRINCIPLES OF THE IT & ACCEPTABLE USE POLICY

All users must act lawfully, professionally, and securely when using MHA systems.

Applies to: All employees, contractors, temporary staff, board members, and any person with access to MHA systems, applications, or data.

This ethos ensures consistent, respectful, and professional conduct across all digital systems.

6. SCOPE

This policy applies whenever you use:

- MHA-issued laptops, mobiles, or tablets
- MHA accounts (email, Teams, SharePoint, etc.)
- MHA networks, WiFi, VPN, cloud services, or applications
- Personal devices used to conduct MHA business

7. DEFINITIONS

User – anyone granted access to MHA systems or data.

IT Facilities – all hardware, software, accounts, networks, and communications systems owned or operated by MHA.

Personal Data – information relating to an identifiable individual, protected under UK GDPR.

8. GENERAL RESPONSIBILITIES

All Users must:

- use MHA IT facilities responsibly and lawfully
- protect MHA's data, reputation, and information security
- act professionally in all digital communications
- comply with UK GDPR, information security requirements, and this policy
- immediately report any loss, compromise, or suspicious activity

If unsure, seek advice from the Executive Officer or a member of the Leadership Team.

9. COMMUNICATION STANDARDS

Users must ensure communications reflect MHA's values and professional standards. They must not harm MHA's reputation and do not disclose personal data improperly.

All communications must be appropriate, respectful, and lawful.

Users must not represent or commit MHA unless authorised or use personal email for MHA business or create personal accounts using MHA email unless approved.

10. INFORMATION SECURITY REQUIREMENTS

MHA is committed to maintaining compliance with the UK Government's Cyber Essential standard. MHA implement appropriate technical controls to protect our systems, data and users from common cyber threats, including secure configuration of devices, firewall protection, access controls, malware protection and regular security updates.

All employees, contractors and third parties must adhere to these controls and use IT systems responsibly, including safeguarding passwords, using MFA where required, reporting suspicious activity promptly and ensuring devices are locked when unattended. Failure to comply with cyber security requirements may result in disciplinary action and could expose MHA to significant risk.

10.1 Passwords & Access:

- Use strong passwords
- MFA (Multi Factor Authentication) where available
- Never share credentials
- Lock screens when leaving your desk
- Use only authorised systems

10.2 Device Protection

Users must ensure protection of MHA devices at all times.

- Protect devices from loss
- Avoid storing MHA data on personal devices
- Secure home WiFi and workspaces

11. REPORT IMMEDIATELY

Users must immediately report instances of suspected phishing, lost/stolen devices, data disclosure, suspicious activity.

If unsure, seek advice from the Executive Officer or a member of the Leadership Team.

12. PERSONAL USE

Permitted if minimal, lawful, and not interfering with duties.

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

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

Employees are permitted to use MHA's 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). The use of chat rooms, eBay and gambling sites is strictly prohibited. The parameters for use of the above are:

1) Personal email messages kept to a minimum.

2) Prohibiting use of email for entering contractual commitments, financial, commercial or private business use.

3) Staff must ensure that messages are not offensive, abusive, defamatory, obscene, discriminatory or harassing.

4) Prohibit access of inappropriate and illegal material, including pornography.

5) No unauthorised software, hacking, bypassing security, malware, offensive material, chain mail, unapproved cloud storage, etc.

13. FILE SHARING & STORAGE

Use only MHA-approved systems (SharePoint, Teams, HomeMaster, CPL).

Do not use Dropbox, Google Drive, or personal email unless permission is obtained.

14. MOBILE PHONES

MHA-issued phones are for business use.

15. NON-COMPLIANCE

May result in loss of access, retraining, disciplinary action.

16. EQUALITY & HUMAN RIGHTS

MHA's is committed to equal opportunities, and we will respond to the different needs and service requirements of individuals, and we will

not discriminate against any individual for any reason outlined in Equality & Human Rights Legislation.

17. DATA COLLECTION

MHA will manage all personal data in accordance with our obligations under the GDPR regulations and the Association's Policy. Further information can be found in MHA's GDPR Policy.

18. POLICY MONITORING & REVIEW

The IT & Acceptable Use Policy will be reviewed by the MHA Board on a three yearly basis in line with EVH updates, or as otherwise deemed necessary.

Milnbank Housing Association
Equality Impact Assessment Tool

Milnbank Housing Association
53 Ballindalloch Drive, Glasgow G31 3DQ

Name of the policy / project proposal to be assessed	IT & Acceptable Use Policy	Is this a new policy /proposal or a revision?	This Policy replaces a previous Policy
Person(s) responsible for the assessment	Pauline Munro, Executive Officer		

1. Briefly describe the aims, objectives and purpose of the policy / proposal	This policy defines how MHA systems and communication tools must be used to protect people, reputation, data, and organisational operations.
2. Who is intended to benefit from the policy/ proposal? *(e.g. applicants, tenants, staff, contractors)*	All employees, contractors, temporary staff, board members, and any person with access to MHA systems, applications, or data
3. What outcomes are wanted from this policy/ proposal? *(e.g. the benefits to customers / benefit to staff)*	All users must act lawfully, professionally, and securely when using MHA systems. Users are aware of responsibilities and procedures to ensure a safe digital working environment. This ethos ensures consistent, respectful, and professional conduct across all digital systems.

4. Which protected characteristics could be affected by the proposal? (*tick all that apply*)

☐ Age ☐ Race ☐ Disability ☐ Marriage & civil partnership ☐ Pregnancy / Maternity

☐ Religion or belief ☐ Sex ☐ Gender reassignment ☐ Sexual Orientation

5. Which other characteristics could be affected by the proposal? (*tick all that apply*)

☐ Socio-economic ☐ Geographic Location ☒ Literacy & Numeracy ☐ Carers ☐ Migrant Status

☐ Single Parents ☐ Families ☒ Other (including Human Rights), please state: Persons who are unable to read may be impacted

6. Have you consulted on the potential impacts of the policy/proposal? (this could be internally with other staff, or externally with customers, focus groups etc)

☒ Yes ☐ No

If yes, provide further details, of who was consulted: Consulted internally with staff from across teams to review the needs of their target audience around communication.

	Positive impact(s)	**Negative impact(s)**
7. Describe the likely positive or negative impact(s) the policy/proposal could have on the groups identified in part 4 & 5.	This policy brings MHA practices up to date based on new internal digital advances.	None.
8. What actions are required to address / mitigate the impacts arising from this assessment? *(This might include; collecting additional data, putting monitoring in place, specific actions to mitigate negative impacts).*	This ethos ensures consistent, respectful, and professional conduct across all digital systems. Free digital IT classes are available.	
Decision / Outcome (Pending Committee Approval)	☒ Approved, no changes required (no impact) ☐ Approved after changes made ☐ Approved with no changes (despite impact) ☐ Stop the Policy . Proposal	

Signed: Patrice Munro Job title: Executive Officer

Date the Equality Impact Assessment was completed: 03.03.2026