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

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

PASSWORD SECURITY 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

PASSWORD PROTECTION POLICY

CONTENTS

1. MHA's Strategic Objectives
2. MHA's Values
3. Regulatory & Legislative Compliance
4. Policy Introduction
5. Principles Training & Development Policy
6. Password Guide
7. Password Protection Standards
8. User Account Deletion and Suspension
9. Breach of Policy
10. Equality & Human Rights
11. Data Collection
12. Monitoring & Review of Policy

1. MILNBANK HOUSING ASSOCIATION (MHA) 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's VALUES

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

3. LEGAL & REGULATORY 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 Governance & Financial Management Standard 6, Risk Management and Internal Controls and Standard 2, Accountability. MHA adheres to all relevant legal employment requirements associated with this policy.

4. POLICY INTRODUCTION

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MHA's entire corporate network. As such, all MHA's employees (including contractors and vendors with access to MHA's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.1 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.

5. PRINCIPLES OF THE PASSWORD PROTECTION POLICY

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that results at the MHA, has access to the MHA network, or stores any non-public MHA information.

6.0 PASSWORD GUIDE

Each system that Users have access to will guide them on when passwords are required to be reset and the format they should be in. Users should ensure passwords are strong and secure and each system guides you through this process.

A general guide - user-level and system-level passwords must conform to the guidelines described below.

Poor, weak passwords have the following characteristics:

- The password contains less than 7 characters
- The password is a word found in a dictionary
- The password is a common usage word
- Contains personal information (addresses, phone numbers)
- Patterns like abcdef, 123456, qwerty

Strong passwords have the following characteristics:

- Contain upper- and lower-case characters
- Contain digits and punctuation
- Are at least 8 characters long
- Are memorable but hard to guess

7. PASSWORD PROTECTION STANDARDS

All passwords should be treated as sensitive and confidential MHA information should be kept private unless evidently reasonable circumstances exist for it to be communicated to other parties.

- Do not use the same password for MHA accounts as for other non-MHA access.

- Do not share MHA passwords with anyone.
- Do not reveal passwords by phone, email or conversation.
- If an account or password is suspended or has been compromised, it must be reported.

If a password is suspected to have been compromised the incident should be reported to the Executive Officer or a member of the Leadership Team or our IT Support Agent and the password changed immediately.

8. USER ACCOUNT DELETION OR SUSPENSION

All User Accounts that are no longer needed must be deleted or suspended immediately.

When a User Account is no longer needed the Executive Officer should be advised immediately.

9. BREACH OF POLICY

Any employee found to have breached this policy will be subject to investigation in accordance with Milnbank Housing Association's disciplinary procedures that may ultimately result in action up to and including dismissal without notice.

10. 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.

11. DATA COLLECTION

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

12. POLICY MONITORING & REVIEW

The Password Protection Policy be reviewed by the MHA Board on a 3 yearly basis in line with EVH updates, or as otherwise deemed necessary.

Milnbank Housing Association
Equality Impact Assessment Tool

Name of the policy / project proposal to be assessed	Password Protection 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	Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of MHA's entire corporate network.		
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)*	The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.		

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.		
7. Describe the likely positive or negative impact(s) the policy/proposal could have on the groups identified in part 4 & 5.	**Positive impact(s)** This policy brings MHA practices up to date based on new internal digital advances.	**Negative impact(s)** 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. Tenants and other customers have access to information in a number of ways. 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