Policy: Mobile Device Management

MUIRHOUSE HOUSING ASSOCIATION

Title of Policy:	Mobile Device Management
Date of Adoption or Last Review:	24 September 2018
Lead Officer:	Grit Nielsen, Corporate Services Team Leader
Date of Next Review:	September 2021

1. Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for Muirhouse Housing Association ("MHA", "us") and support us in achieving high standards of efficiency and service. However, mobile devices also represent a risk to data security as, if the appropriate security applications and procedures are not applied, this could lead to unauthorised access to the MHA's data and IT infrastructure. This could subsequently lead to data leakage, loss of personal data, breach of the data protection regulations and system infection. MHA has a requirement to protect information assets in order to safeguard our customers, intellectual property and reputation. This policy outlines a set of practices and requirements for the safe use of mobile devices and applications.

2. Scope

Mobile devices may only access the corporate network if they are owned by MHA. Mobile devices include mobile phones, smartphones and tablet devices. The scope of this policy does not include laptops.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be carried out and authorised by one of the Authorised Approvers; The Corporate Services Team Leader, the Finance & Corporate Services Manager or the Chief Executive.

Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

Breach of this policy may lead to disciplinary action in line with our Disciplinary Policy.

3. Policy

3.1 Technical Requirements

All MHA devices must use the following Operating Systems: Android 2.2 or later, Windows 7 or later.

Devices must be configured with a secure password that complies with MHA's password policy. This password must not be the same as any other credentials used within the organization.

- Mobile phone devices must have a pin as password as this is the most secure form of protection hacking.

- All tablet devices must have a password login to the system that agrees with the following rules:
    - A minimum of 8 characters long
    - A mix of at least 3 out of 4 of the following: capital letters, lower case letters, numbers, special symbols.

Only devices managed by our IT provider will be allowed to connect directly to the internal corporate network. These devices will be subject to the valid Group Policies on security features such as encryption, password, key lock, etc. These policies will be enforced by our IT provider using Mobile Device Management software.

3.2 Staff Requirements

Staff must report all lost or stolen devices to the Corporate Services Team Leader immediately.
If a staff member suspects that unauthorised access to Association data has taken place via a mobile device, they must report the incident to the Corporate Services Team Leader immediately.
Devices must not be “jailbroken” or “rooted”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

Staff must not load pirated software or illegal content onto their devices, and applications should only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact our IT provider.

Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied as soon as it is possible to connect the device to WiFi.
Devices must only be connected to a PC which is managed by our IT provider.

Staff must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify the Corporate Services Team Leader immediately.

MHA is entitled to check the above requirements if there are grounds for suspecting a breach and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
Should a device wipe be performed, the user is responsible for the backup of their own personal data and MHA will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

Staff must not use corporate workstations to backup or synchronise device content such as media files, unless such content is required for legitimate MHA business purposes. Corporate workstations and devices must never be used to backup and synchronise personal cloud services.

**To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.*

3.3 Staff Care Requirements

Staff must handle their devices with care and respect and a protective sleeve should always be used when transporting a tablet device.
Staff must never leave their devices unattended in a car or in a customer's home. In the office devices must be locked away at night and during the weekend when the office is closed.

Staff working from home must take care to keep their devices safe and to ensure they are not accessed by other members of the household.

3.4 Use of particular applications which have access to corporate data

MHA supports the use of the following cloud storage solutions:

- OneDrive through Office 365

The use of solutions other than the above are subject to approval from one of the Authorised Approvers; The Corporate Services Team Leader, the Finance & Corporate Services Manager and the Chief Executive.

4. Review of Policy

This Policy will be reviewed in three years or sooner if significant changes are required.