Mobile Device Policy

Introduction

The Michael Lonsdale Group inclusive of Michael Lonsdale Ltd, Michael J Lonsdale Ltd, Michael J Lonsdale (Electrical) Ltd and E7 Building Services Ltd (Michael Lonsdale) recognises that mobile devices such as smartphones and tablet computers are important tools for employee's productivity. While efficient and a major part of today's working culture, when using mobile devices there are inherent data security risks that should be mitigated where possible.

This document outlines the Michael Lonsdale mobile device policy to ensure best practices are adhered to when using mobile devices for company business, regardless of the location.

Please note, this policy document covers working specifically with mobile devices remotely and the security precautions required. For further information on Remote Working and the processes to request it, please refer to the **Remote Working Policy**.

The responsibilities in this document cover both mobile devices owned by Michael Lonsdale or the employees' own devices if they are used to access company used platforms or services. These services include the use of systems such as Microsoft 365.

Scope

This policy applies to the directors, employees (full-time, part-time, or casual), volunteers and subcontractors of the Michael Lonsdale Group.

The Michael Lonsdale Group policy and procedure documents may be distributed to suppliers, accreditation bodies, compliance bodies and any other relevant third parties.

In some cases, third parties such as suppliers or those performing on-site work or through our online presence for the Michael Lonsdale Group will be expected to adhere to our policies, which will be made available where applicable.

We will review and update this policy adhering to our data protection obligations. It does not form part of any employee's contract of employment, and we may amend, update, or supplement it from time to time.

We will circulate any new or modified policy to employees and any other stakeholders when it is adopted.

Definitions

Mobile phones are defined as any smartphone, other mobile phone types and variants of mobile phones, such as tablets and gaming devices with or without internet connectivity.

Mobile devices include laptops, whether provisioned to employees by Michael Lonsdale or personal devices.

Remote working is defined as any location outside of the Michael Lonsdale Group offices.

Policy

Employees using a company or their own mobile devices to perform business tasks (such as reading and responding to email or accessing SharePoint) must ensure that:

- The devices are secured with suitable passwords, passkeys, PIN or at least biometric (fingerprint/facial recognition) access.
- Devices must be kept up to date with the latest mobile operating system releases (Android/iOS etc).
- If devices used to access the Michael Lonsdale Group services are lost that the loss is reported to Michael Lonsdale management or our third-party Managed Services Provider (“MSP”) D H Technical Services Limited (DHTS) immediately - even if it was the employee's own device.
- They do not use rooted or jailbroken devices to access Michael Lonsdale services.
- They do not load pirated or illegal software onto devices that are intended to be used for work purposes.
- Due care is taken when sending emails from personal devices ensuring that personal and work emails are not confused or merged.
- They never attempt to access server environments or connect to client networks on their own devices without using Windows SSTP VPN.
- They never download company data onto personal devices.

Remote Working

Home/Remote Working Definitions

Home/Remote Working	Is defined as any work outside of the Michael Lonsdale office space such as working in collaborative spaces, in public, at home or whilst in transit.
Public Spaces	Any environment where there is no control over access or data connection, for example, cafes, airport lounges and so forth.
Unsecure Public Space	Any public space where there is a high risk of being overlooked or overheard, for example densely populated cafes, buses, trains, and other public spaces.
Private Spaces	Any environment outside the Michael Lonsdale Group, where there is control over the access or data connection, for example, the staff member's home, private collaborative workspace and so forth.
Secure Data Access	Any access to data wholly through: • A network under the control of the individual (e.g., password-protected home Wi-Fi, password-protected mobile "hotspot", personal VPN, etc) • Public networks with individually assigned passwords.
Unsecure Data Access	Any access via non-password protected Wi-Fi networks without the use of a VPN.

Device Security

The Michael Lonsdale Group support remote working and has provisioned our employees with Laptop computers and mobile telephones that are secured with:

- Endpoint Security software is installed on all devices
- Managed by Microsoft Intune.

Remote access to any on premises environment is done via Windows SSTP VPN only.

Security – Home/Remote Environments

- Due care and attention to household security should be paid, including securing devices and laptops particularly when being left unattended.
- Devices or laptops should not be left in a vulnerable position, for example in public view.
- Devices that are logged in to the Michael Lonsdale Group services should not be shared with or accessible to other members of the household or other parties.
- A clear desk policy should apply when away from an office location. This means that personal information on Michael Lonsdale people or staff should not be available for others to view.

Working in a Public Environment

Physical Security – Public Environments

- Laptops or other devices should always be secured or kept on the person when working in such environments. Under no circumstances should laptops or other devices be left unattended, even for a short period – this includes being left in a locked vehicle.
- Due care and attention to all other belongings such as bags, printed documents or other personal work items should be exercised, and these should be treated the same as laptops and other devices.
- Device screens should be locked whenever necessary and should have an automatic timeout enabled.

Information Security

- Due care and attention should be paid to your surroundings.
- In public spaces, eavesdropping should be considered before making any sensitive calls.
- All staff should use a privacy screen where sensitive data is being viewed.
- Staff must not use open/unsecured Wi-Fi locations or hotspots when accessing information.

Usage

Employees using company or their own mobile devices to perform business tasks (including reading emails) must also ensure:

- If using their own device(s), employees do not download any company or 3rd party information onto the device hard drive or removable media.
- Any access to corporate data must be through the provisioned cloud-based systems or Windows SSTP VPN.
- If required for part of a task then the data must be fully deleted immediately after use.
- They do not use open/unsecured WiFi locations or hotspots when accessing any company information.
- They do not leave devices, especially unlocked, in public places.
- They do not share login credentials or other access information with other individuals from within or without the company.
- They use the same due care and attention to when opening email attachments and downloading data that they do with home and work computers.
- When being transported, mobile devices as well as being locked/password protected should always be within sight of the employee or on their person and never left unattended.

The Michael Lonsdale Group Devices

- Company devices should only be used for work-related actions, including website browsing.
- The devices should never be used to view or send offensive or illegal material.
- The devices should not be used to visit non-work-related sites or applications such as games and media viewing.
- The devices should never be tampered with in respect of the operating system software or any protection controls, such as Bitdefender, removed or disabled.
- They will always be kept up to date with the latest operating system updates for security reasons.

MICHAEL LONSDALE GROUP

Due care for personal and company devices. The following points are guidelines to protect users and Michael Lonsdale from security breaches concerning mobile devices:

- Do not have auto Wi-Fi connect on to unsecured hotspots.
- Do not leave devices, especially unlocked, in public places – for example on trains when temporarily away from the seat or in eating locations, especially on tables.
- Do not share login credentials with anyone, even those that work for Michael Lonsdale unless performing IT updates or similar services to repair or update the device.
- Use the same due care and attention when opening attachments to emails and clicking links in text messages that are from unverified sources.

Name: G Herbert For and on behalf of the Michael Lonsdale Group

Position: Managing Director

Signature: 

Date: 8th Sept 2022