NetFM UK

Information Security – Mobile Devices Policy

1. Intended Audience & Use

This policy describes the rules covering use of mobile computing devices by NetFM employees, or that are used to host NetFM Information (or information owned by NetFM clients).

This includes, but is not restricted to, Personal Digital Assistants (PDA's), tablets, Smartphones, Mobile phones and Blackberry handheld devices.

It applies to NetFM employees and all other parties who are given access to NetFM data, including NetFM staff,
business users, NetFM technology providers, independent producers,
contractors, freelancers and agents.

2. Objective & Scope

2.1 Objective

Business use of mobile telephony devices with data hosting and processing capabilities has increased dramatically in recent years. The increasing ubiquity of smartphone devices means that any policy must also cater for the possibility of employee-owned devices being used to host, send and receive NetFM data.

This policy sets out principles that must be adhered to when using mobile devices to connect to NetFM networks or to access or host NetFM data or that of NetFM's clients. These are designed to ensure that NetFM data is adequately protected from unauthorised access, both at rest and in transit over data networks, and to help ensure compliance with the Data Protection Act.

If you use a mobile device (either your own or NetFM provided) to store or transmit NetFM data, it is vital that you read this policy carefully.

If there is anything you do not understand, it is your responsibility to ask the Technical Director for clarification.

If you fail to comply with this policy you may be subject to NetFM's disciplinary procedures and / or legal proceedings. Your failure to comply may also result in legal proceedings against NetFM and/or result in your dismissal.

2.2 Scope

All mobile computing devices (whether personally owned or NetFM provided) used to receive, store and/or transmit NetFM data.

This includes, but is not limited to: Blackberry handhelds, smartphones, laptops, netbooks, tablet PCs, USB flash/hard drives, removable media and portable digital assistants (PDAs).

This policy sets out high level, generic security requirements – it does not include any platform-specific configuration requirements. Where such requirements are defined in a more specific NetFM standard, you are expected to adhere to that standard in conjunction with this policy.

3. General Policy Statements applicable to NetFM-Owned Devices

Applicable policy statements are categorised below:

3.1 Audit and Monitoring

All NetFM supplied mobile devices and their contents remain the property of the corporation and are subject to regular audit and monitoring.

3.2 Connecting to non-NetFM equipment

In order to protect the NetFM from malware, you must not connect NetFM owned mobile devices to your home computer unless that computer:

- is running an up to date anti-malware product.

- is up to date with recent operating system and application security patches.

3.3 Data backup and synchronisation

NetFM data stored on the device should be regularly backed up to a secure location on NetFM equipment or network to minimise impact of data loss in the event of a hardware failure. (Minimum of every 3 months but we would advise much more frequently if you use your device as sole repository for business data you generate).

NetFM owned devices should preferably be synchronised only to NetFM equipment, to ensure that NetFM data is not synched or backed up to devices that are insecurely configured, and to reduce the risk that the device becomes infected with malware.

Where there is a business requirement to synchronise NetFM data to non-NetFM equipment, care should be taken to maintain the security of that data1. Restricted or Confidential data must be protected as per the requirements of NetFM's other Data & Information Security Policies.

3.4 Compliant Device Configuration

NetFM devices on certain managed services are supplied pre-configured in a compliant state. Once received the employee is not authorised to change any security device settings without authorization from the Technical Director, as they may affect the security of the device, or stop it functioning with the supplied service. (This does not apply to resetting the PIN).

NetFM devices on other services may not be supplied pre-configured in a compliant state, depending on the service being offered. Advice should be sought from the Technical Director as to how to configure such devices to comply with this policy and any device-specific NetFM standards.

3.5 Loss / Theft and Physical Security

If a NetFM owned device – or any employee-owned device that holds NetFM data - is lost or stolen, then the Technical Director should be contacted as a matter of urgency, so that the NetFM data network can be protected from the device and to enable it to be remote wiped where that functionality exists.

Physical security – The device must be kept securely at all times. For example it should never be left unattended in a car, in a hotel room (except in a safe) or on the floor of a bar or restaurant in a bag or at home (visible through window).

For example, mobile phone backup tools bundled with synchronisation software are increasingly offering encrypted backup functionality. Access to such backups could then be secured using a strong password.

Please refer to the NetFM Password Policy document before contacting NetFM's Technical Director for specific advice.

3.6 Installation of Software (on the mobile device)

You must not install any software unless you have a licence that is valid for commercial use. It is your responsibility to verify that the licence allows commercial use prior to installation – this includes any applications purchased from online mobile application stores.

Please note for NetFM laptops, you should not be installing software yourself – this should be requested via the appropriate route, and the details of licenses purchased should be reported to the Technical Director for recording.

4. General Policy Statements applicable to User Owned Devices

Applicable policy statements are categorised below:

4.1 Connecting to NetFM equipment, networks and services

Devices connected to NetFM networks must be scanned for malware each time they are connected, using NetFM's desktop anti-malware software. Any files copied from the device to the network must be individually scanned before e-mailing them on, storing them on a NetFM data area or uploading them into a NetFM system.

Only devices which have been configured to comply with this policy and with any device specific NetFM published standards and/or standards from approved suppliers, may be connected to NetFM's Mobile E-mail Service (MES) or used to host "Private Internal" or "Confidential" Data.

4.2 Connecting to non-NetFM equipment

Where you have a business requirement to connect a user owned mobile device to NetFM networks and equipment, you must ensure that any other (non-NetFM) equipment that you connect that device to:

- is running an up to date anti-malware product.

- is up to date with recent operating system and application security patches.

4.3 Data Backup and Synchronisation

You are strongly advised to regularly back up your phone to ensure that your contacts and other data/applications can be recovered in the event of device failure or loss. Phones usually come with software that allows them to be backed up to your PC. Such software should not be installed on a NetFM computer unless it has been integrated with the NetFM desktop.

Where NetFM owned data is stored on a user owned device, that data must not be backed up to non-NetFM equipment where that data is restricted data, unless it is secured as required by NetFM's Information Security Policies.

4.4 Loss/Theft and Physical Security

If a user owned device containing any NetFM data is lost or stolen the Technical Director should be informed immediately.

If you are using a NetFM service which allows the device to be remote wiped, this should be actioned by informing the Technical Director.

Physical security - Where NetFM owned data is stored on a user owned device, that device must be kept securely at all times. For example it should never be left unattended in a car / on public transport, in a hotel room (except in a safe) or on the floor of a bar/restaurant in a bag or at home (visible through window).

5. Phone Type Device Configuration Policy Statements

These generic configuration policies must be adhered to:

As a condition for attaching your phone (or telephony capable mobile device) to certain NetFM data services. (E.g. The NetFM's Mobile E-mail Service - MES); and/or

Where the device is used to store or host "Private Internal" or "Confidential" Data.

Where an approved platform specific configuration standard exists – that must be complied with.

Where functionality referred to does not exist for your device – refer to the approved platform specific configuration standard for applicable policies and guidance.

5.1 Encryption

Phone memory encryption must be enabled.

Insertable memory card encryption must be enabled.

Please refer to the NetFM's Information Security Policy for specific policy guidance on how to protect "Private Internal" or "Confidential" Data with encryption.

5.2 Device Locking

Device lock must be enabled with a PIN of at least 6 digits (this should both include letters and numbers where supported) or a swipe pattern that uses at least 6 nodes.

Device lock must be set to autoengage after a maximum of 5 minutes.

SIM lock should be enabled with a PIN of at least 4 digits. 6 digits are recommended.

Device lock and SIM lock codes must be required on phone boot in order to access phone functions and data.

5.4 Anti-malware

This is not currently required to be installed on the phone.

This requirement refers to encryption services provided by the device, not third party encryption tools like Checkpoint.

Jailbreaking refers to the practice of unlocking a device to enable root access and installation of applications from outside of authorised repositories. It increases the risk of malware infection on a device and is not advised.

Any applications downloaded must be scanned for malware prior to installation except where the store's application review policy clearly asserts that this is covered.

5.5 Remote disablement and wiping

Remote wipe functionality must be configured where it is available on NetFM owned devices.

Remote wipe functionality should be configured on personal devices where it is available – the device owner will be required to sign a waiver agreeing that NetFM may action a remote wipe on a personal device if and when it is deemed necessary by NetFM, and only where authorised by the NetFM Technical Director.

Where technically feasible, only NetFM data will be wiped, but it may be necessary to wipe ALL data. The device owner will be responsible for backing up all personal data on the device to ensure the minimum data loss should remote wiping be required.

Remote SMS locking functionality should be configured where it is available. (This functionality allows you to preset an alphanumeric code which when received as the sole component of an SMS message, will immediately lock the phone – requiring PIN entry to unlock.)

Incorrect password entry functionality should be configured to wipe the device after a maximum of 8 incorrect password entry attempts.

5.6 Touchscreen devices only

Where available password/PIN entry mode should be configured to use a secure entry mode where the position of the characters on screen changes each time you log on.

6. Functionality dependent policies

This section contains policy statements that are only applicable to devices where the relevant functionality exists.

6.1 Specific points on the use of mobile devices with camera functionality

NetFM owned mobile devices enabled with cameras should primarily be used for taking business related pictures. Some limited personal use is allowed, but storage must not interfere with NetFM business use.

Inappropriate content prohibition on NetFM owned devices applies equally to mobile phones as it does other forms of communication.

Privacy, only take pictures of individuals with their permission to do so, or follow current policy where this is impractical.

Photographs taken for business reasons are recommended to be backed up to the NetFM data network as soon as possible to prevent the risk of the data being lost should the device fail.

6.2 Specific points on the use of Bluetooth enabled devices (NetFM owned devices only)

Bluetooth must only be used for accessing passive devices – such as hands-free kits.

Bluetooth cannot be used to communicate with a device directly connected to the NetFM data network.

Bluetooth connections must be accepted from other devices with care. Ensure the recipient is known and agree connection security criteria in advance.

Never run a NetFM device in broadcast mode as various viruses and other schemes are prevalent whilst in this mode.

6.3 Specific points on the use of Infrared enabled devices (NetFM owned devices only)

Infrared must only be used for accessing passive devices, no sync should be performed using the interface.

Infrared cannot be used to communicate with other devices, and should be turned off.

No NetFM data can be sent to other devices (including NetFM owned ones) using the Infrared protocol.

7. Non phone-based mobile computing devices

This section contains policy statements relating to mobile computing devices other than mobile phones/smartphones. It is organised by category.

7.1 Laptops / Netbooks

Use of Full Disk Encryption products (standard on NetFM desktop) is required as a condition for hosting “Private Internal” or “Confidential” Data. See NetFM Data Classification Policy for more detailed requirements.

User owned laptops/netbooks may not be connected to the NetFM network – except limited access available via NetFM Webmail.

7.2 USB attached data storage

This includes portable hard disks, flash or thumb drives and memory cards in digital devices (e.g. cameras/photoframes/mp3 players).

“Private Internal” or “Confidential” data must not be stored on these devices unless an encryption method compliant with the NetFM’s Information Security Policies is used to protect it.

Devices must be scanned with the corporate anti-virus solution prior to copying any files to or from them.

7.3 Digital music/video players (e.g. iPods)

If the device is NetFM owned, and you choose to store personal music or video (ie media that is not owned by the NetFM), this must not be synched to the NetFM data network.

NetFM owned media content must not be stored solely on personal devices. Care should be taken to ensure the security of such material.

Digital music/video player devices should normally be connected in "Mass Storage" mode and scanned for malware at the point of connection. Synchronisation software that has been integrated for the NetFM desktop can be used. Depending on the product - installation may be subject to approval by the Technical Director.

7.4 Removable Media

This includes Blu-ray discs, DVDs, CDs, floppy disks, tapes and Iomega Zip/Jazz cartridges or equivalent.

Restricted data must not be stored on removable media unless an encryption method compliant with the NetFM’s Information Security Policies is used to protect it.

8.0 Wifi Hotspots

NetFM owned devices – or employee-owned devices holding NetFM data - are not to connect to the NetFM network using public unverified wifi hotspots.

Similarly, do not connect to a NetFM client’s network over a public unverified wifi hotspot.

9.0 Remote Working

All employees, working in a public place, whether on mobile devices or otherwise, must be mindful of working on or discussing sensitive business matters in public places.

This especially refers to discussing work, or details of work, that may be considered “Private Internal” or “Confidential” data – as laid out in the NetFM Data Classification Policy.