Mobile Device Policy

Version 1 May 2018

The purpose of this policy and procedure is to ensure that employees are aware of their responsibilities when using mobile device equipment provided by Manchester Metropolitan University. Mobile telephones and tablets are referred to, as "mobile devices" in this document.

Scope

This policy applies to:

1. All permanent and temporary employees and any other third parties using equipment provided by Manchester Metropolitan University.
2. All forms of mobile devices within the University including, but not limited to all mobile phones including non-internet connected devices, all tablets including Wi-Fi and sim-connected devices (excludes laptops).

Policy Statement

The practices and procedures set out in this document reflect the provisions set out in the Computer Misuse Act 1990, the Data Protection Act 1998, the General Data Protection Regulation (as of May 2018), the Malicious Communications Act 1998, the Road Vehicles (Construction and Use) (amendments) Regulations 2003 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Objectives

The objectives of this policy:

1. Define and set out the appropriate use of mobile devices.
2. Ensure the protection of information held on or accessible from mobile devices.
3. Ensure the University minimises the threat of accidental, unauthorised or inappropriate access to electronic information owned by the University or information temporarily entrusted to it.
4. Provide guidelines for professional use of mobile devices, to ensure the devices are used in such in a way that does not compromise the University or its employees in any way.
5. Detail the mobile devices available to order, the process for obtaining a device and monthly costs associated with a mobile device.
6. Set out possible outcomes if the mobile device is used incorrectly and what process to follow if a device is lost or stolen.

Requirements

1. Users must be aware of their responsibilities when using mobile devices provided by the University.
2. Users must be aware of the bounds of personal use and the seriousness with which the University views the inappropriate, excessive, unlawful or malicious use of the mobile devices provided.

3. Users are expected to observe the arrangements set out in this policy and to report any circumstances where they believe mobile devices are not being used appropriately to line management or the IT Helpline on 0161 247 4646 or it.helpline@mmu.ac.uk

4. Where a mobile device allows access to the internet, any use of that facility is governed by the following University policies:

    a. ***Information Security Policy***
    http://www2.mmu.ac.uk/isds/information-security/policies/is/
    b. ***Information Risk Management Policy***
    http://www2.mmu.ac.uk/isds/information-security/policies/risk-management/
    c. ***Data Protection Policy***
    https://www.mmu.ac.uk/policy/policy.php?id=100
    d. ***Mobile and Remote Access Control procedure***
    http://www2.mmu.ac.uk/isds/information-security/policies/remote-access/
    e. ***Acceptable Use of University IT Systems***
    http://www2.mmu.ac.uk/isds/information-security/policies/acceptable-use/

5. The user should take reasonable steps to prevent damage or loss to their mobile device. This includes not leaving it in view in unattended vehicles and storing it securely when not in use. The user may be responsible to the University for any loss or damage if reasonable precautions are not taken.

6. Users must not re-allocate mobile devices to others without first seeking authorisation from ISDS, this can be requested via the IT Helpline 0161 247 4646, it.helpline@mmu.ac.uk. In the event this change is authorised, all elements of the contract including phone number will also be transferred, and should be acknowledged and signed for by the users. The transfer will be managed by the Business Support Team to ensure the system is updated with the new owner's information.

7. The mobile device is, at all times, the property of Manchester Metropolitan University and must be surrendered on request for any reason. The University has the right to access content on mobile devices, cross-referencing the ISDS Acceptable Use policy: http://www2.mmu.ac.uk/isds/information-security/policies/acceptable-use/

8. Mobile devices have the capability of taking still or moving images. This represents a potential threat to the privacy and dignity of those both internal and external to the University. No still or moving images of individuals may be taken without their express consent. Images of properties may be taken on estate visits or property inspections with mobile devices but these must not include identifiable images of individuals without their express consent first being obtained. No still or moving images taken with the University mobile devices are to be posted onto the internet / social media sites without appropriate authority being first obtained.

9. The University discourages the use of mobile devices whilst driving. Where a driver must take a call they should ensure that they comply with the current legal position and ensure that any hands free device used is legally compliant. On no account should any University employee use mobile devices other than hands free whilst driving. Conference calls should not be conducted whilst driving.

Acceptable use

All employees are expected to use mobile devices provided by the University in an appropriate, acceptable and reasonable manner in accordance with the University's Acceptable Use of University IT Systems Policy. Employees are expected to exercise good sense and responsibility in limiting any personal use of their mobile devices to a minimum and refrain from any inappropriate use. The following list gives (non-exhaustive) examples of inappropriate use of University mobile devices:

1. Communications to premium rate numbers
2. Communications to votes of TV/radio programmes
3. Communications involving bidding in online auctions
4. Communications to betting sites/competitions
5. Communications that are illegal, obscene, libellous or slanderous
6. Communication that are offensive or threatening
7. Communications that infringe copyright
8. Communications that transmit unsolicited commercial or advertising material
9. Communications that transmit spam, chain or junk messages
10. Any other use that might cause commercial, reputational or financial distress to the University
11. Excessive use (including excessive use both within and outside of the user's working hours)
12. Any communication or action, which would contravene the University's Acceptable Use of University IT Systems policy, or any other University policy

Users are reminded that emails, text messages and any communications sent on University mobile devices are admissible in court and subject to Data Protection and Freedom of Information, legislation and therefore they could be released into the public domain or to individuals mentioned in them.

Users found using their mobile devices in an inappropriate manner might have their mobile devices withdrawn and be subject to disciplinary action under the University's Disciplinary Procedure (or other relevant procedure).

Cost and usage is monitored and where excessive personal use is identified, costs may have to be reimbursed to the University. The University will determine what constitutes excessive personal use depending on particular circumstances.

Mobile Devices

The University will offer a range of handsets and tablets available to order for staff, via the P2P system. The devices available will be one prior to the latest model. Requests for alternative devices can be sent with a business justification and approval from your department Director to the IT Helpline (0161 247 4646, it.helpline@mmu.ac.uk).

The range of handsets will be one model prior to the latest model i.e. currently iPhone 7 & Samsung 8.

The current device list can be found on P2P, (search for Vodafone supplier catalogue) or on the Mobile Device Operational Policy, which can be found on the ISDS website.

Costs

For current pricing and SIMs available, please refer to the Mobile Device Operational Policy, which can be found on the ISDS website.

The University offers Staff a choice of three SIM only contracts. Mobile phones should be purchased separately at an additional charge. Mobile devices can be purchased via P2P. Only University devices can be used with this SIM card.

Please note, there are no minimum terms for SIM only contracts, however you must let the IT Helpline 0161 247 4646, it.helpline@mmu.ac.uk know when contracts are no longer required or where you propose to transfer it to another staff member.

Line managers are responsible for keeping control of mobile device usage by identifying those individuals who use a mobile device excessively and taking appropriate action.

Bills for mobile devices will be available online via the Vodafone online portal; access can be set-up by the Business Support Team. Billing administrators are responsible for checking departmental bills and approving payment. Bills not queried within 7 days of receipt will be paid automatically. Bill queries should be directed to the Business Support Team.

All connections are automatically barred from international roaming. If you require international roaming this will need to be requested via the IT helpline 0161 247 4646, it.helpline@mmu.ac.uk Please note there is a daily charge for any international roaming outside of the EU and budget holder approval will be required before this can be added to your connection.

Roaming in the EU is now charged at UK data rates however, you will need to check your destination in Europe is in the EU, as charges will apply for countries outside of the EU in Europe. Please note calls made from ships and cross channels ferries will not be covered under the EU roaming policy and will be charged.

It is the responsibility of billing administrators to draw billing issues to the attention of the individual user's line manager. The University's Service Provider will monitor usage charges and when the total for a single device exceeds a predetermined limit, the Business Support Team will be alerted. The Business Support Team will then contact the relevant line manager for approval to continue to increase the user's limit, the line manager to ensure that usage is brought down to an acceptable level, or suspend the service. The Business Support Team will provide all billing administrators with the names of employees in their department for whom they should expect monthly bills for mobile devices.

Insurance

Insurance is required on all mobile devices with a cost over £250 and covers the following:

- Water and liquid damage (including out of warranty cover)
- Loss and theft
- Covered anywhere in the world

Insurance will be arranged by the Business Support team when the order for a new device has been placed.

For the current device insurance available, please refer to the Mobile Device Operational Policy, which can be found on the ISDS website.

Data

Users have the right, under the Data Protection Act, to receive, on written request, a copy of any personal data concerning them, including information held electronically on systems owned by the University including mobile devices. There are a few limited exceptions to this such as data held for crime prevention/detection purposes, but most individuals will be able to have a copy of the personal data held on them. Full details of how employees can obtain such information are set out in the University's Policy on Data Protection.

Safety

Caution should be exercised in the use of mobile devices avoiding long duration phone calls, texting or emailing where possible with regular breaks from screens as needed.

Security

All mobile devices must be password protected and not used in public places without due care and attention by the user.

All lost, stolen, or mislaid mobile devices are to be reported immediately to the IT Helpline 0161 247 4646, it.helpline@mmu.ac.uk as soon as practicable. The user must also report the loss to police as soon as practicable and obtain a case reference number.

All security incidents, including actual or potential unauthorised access to the University's information systems, must be reported immediately to the ISDS Helpline 0161 247 4646, it.helpline@mmu.ac.uk.

Mobile devices that are lost or otherwise compromised through lapses in security by the employee may incur costs in respect of replacement or device or call charges, which will be recharged to the user. The mobile device may be removed at any time if this policy is breached.

Policy maintenance

The University will issue supporting standards, guidelines and procedures on an on-going basis. Employees will be informed of any subsequent changes of this policy by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from the University website or other relevant communication media on an on-going basis and accept the terms and conditions contained therein.