Mobile Computing Policy

1. Introduction

1.1. The purpose of this policy is to maintain the security of De Montfort University's (DMU) information assets when they are used from mobile devices. For the purposes of this policy 'mobile devices' or 'mobile computing devices' refers to devices such as PDAs, mobile phones, laptops, tablets etc. - these devices need not be owned by DMU for this policy to apply if they are being used to access the university's information systems.

1.2. The common term used for devices owned by the user but used to access corporate information is BYOD (Bring Your Own Device). A useful list of BYOD FAQs is in appendix 1 at the end of this document.

1.3. This policy is to ensure that users understand their role and responsibilities when taking DMU equipment and/or data off-site and accessing university systems and services remotely.

1.4. Any exceptions to this policy must be agreed by the Director of ITMS or their designated deputy.

2. Appropriate use of university owned mobile computing devices

2.1. DMU-owned mobile computing devices issued to staff are provided at the discretion of the university on the basis of business need and remain the property of the university at all times. They must be returned to DMU on request, and on termination of employment.

2.2. University-owned mobile devices should be used for the intended purpose and in accordance with the university's other information security policies.

See also the policies on the *Information Security* page.

2.3. The university reserves the right to monitor use of DMU owned mobile computing devices. In using the university's devices, individuals consent to such monitoring. For further information on monitoring see:

- *Policy on the use of email, internet and social media*
- *Network Management Policy*
- *DMU Code of Conduct*

2.4. Any loss of or damage to a device that stores DMU-owned confidential or personal data as defined in the *Information Handling Policy* must be notified to the ITMS Service Desk and the user's line manager as soon as possible.

2.5. Manufacturers' recommended safety instructions regarding transportation and protection against hazards must be observed at all times for university owned devices.

3. Use of personal mobile devices to access university systems and services

3.1. DMU does not require staff or students to store or access DMU-owned personal or confidential information using devices it does not own or manage. The DMU *Information Handling Policy* sets out the university's definition of, commitment to and requirements for information handling.

3.2. Should a member of staff elect to use a device not owned or managed by the university and the device is accessing information classified as 'personal' or a higher classification as defined in the "*Information Handling Policy*", reasonable measures as defined in section 4 below may be taken by the university to ensure the security of that information.

3.3. When using non-university-owned devices to access university systems and services, it is the responsibility of users to ensure that reasonable measures have been taken to secure the device including up-to date anti-virus software and ensuring operating systems and software are up-to-date and secure.

3.4. Appendix 1 contains FAQs about the use of personal mobile devices to access university systems and services.

4. Protecting university data on mobile devices

4.1. The university may take appropriate measures to protect the data or those affected should any data be compromised through loss, damage or disclosure.

4.2. When hand-held devices connect directly to the DMU Staff email system there is a facility to wipe the device. If used, this functionality will wipe not only DMU-owned data but all personal data, including contacts, text messages, accounts, etc. from that device. This functionality is a default part of the Exchange software.

4.3. The remote wipe facility can be used by staff via the Webmail system (in respect of their own devices only) and the ITMS email administration team, in respect of any devices that connect to Exchange. The email administration team will only ever wipe a device with the written permission of the owner of the device or in exceptional circumstances, where it is impossible or impractical to obtain this and where it has been determined by the Director of ITMS or their nominated deputy that it would be appropriate to protect confidential or personal data against unlawful access, such as in the event of the loss of a device. For this reason, it is advised to securely back up any such device on a regular basis.

4.4. For any devices synchronising to the DMU staff email system using the ActiveSync Protocol to communicate with Exchange, whether they are owned by DMU or staff personal devices, following rules are enforced:

- Must have a minimum password length of 4 digits.
- The number of failed password attempts a mobile device accepts before all information on the device is deleted and the mobile phone is automatically returned to the original factory settings is set to 10.
- Time without user input before password must be re-entered is set to 15 minutes

4.5. DMU will not access or monitor DMU data held on a personal mobile device except with the explicit consent of the device owner.

4.6. DMU will not activate Microsoft Exchange policies that allow any access to or monitoring of data held on personal mobile devices.

4.7. Staff should not store or access DMU's personal and/or confidential information in unencrypted format on or from any device not owned by them (See the DMU Encryption Policy), the university or authorised third parties, e.g. partner colleges, partner organisations in research consortia. See Section 2.1 above.

4.8. When travelling, mobile devices should not be left unattended unless unavoidable due to reasonable local requirements e.g. in flight, in restricted security zones.

4.9. Any loss of or damage to DMU data or a potential breach of security should be notified to the ITMS Service Desk (Tel: 0116 2506050, Email: itmsservicedesk@dmu.ac.uk) and the user's line manager as soon as practically possible, and no later than within 24 hours of discovery.
4.10. Staff should not use mobile devices if there is significant risk of harm, loss or damage to the individual or of harm, loss, damage, corruption of the device or of loss, corruption or interception of the data upon it.

5. Breach of the policy

5.1. If a staff member is found to have acted in breach of this policy this may lead to disciplinary action being taken against them, up to and including dismissal.
5.2. Breach of the policy could result in university-owned mobile devices being withdrawn.

6. Responsibility for Information Technology and Security Policy Documentation

6.1. The University Executive Board or its delegated authority has ultimate responsibility for approving updates and additions to the University information technology and security policy documentation set.
6.2. The Information Governance Board is the information security oversight committee. The objective of this board is to ensure that there is clear direction and management support for security issues.
6.3. Proposed changes and additions to the policy documentation may be submitted by any member of staff, via a Dean of Faculty or Director, to the Director of ITMS or delegated authority before consideration at the Executive Board or appropriate sub-committee.
6.4. Proposed updates to policy must be fully converted into proposed changes to the policy documentation. This must be done in such a way that implications for all related documents are fully taken into account

7. Document approval

Approved by: Paul Marshall, Chair of the Information Governance Board
Approved Date:
Review Date:
Reviewer: IT Governance Manager

8. Document history

8.1. 15th December 2010 – Draft 1 Neil Faver
8.2. 5th October 2012 – Version 1 Neil Faver
8.3. 12th August 2016 – Version 5.12 Neil Faver

Appendix 1 – BYOD FAQ's

This appendix is intended to give a snapshot of the current situation with respect to the issues that should be considered by a DMU member of staff before connecting their own mobile computing device to DMU systems.

This appendix is not exhaustive and staff are strongly advised to speak to the ITMS Service Desk (#6050) or their ITMS business analyst for advice if they are in any doubt as to how to proceed.

Do I have to connect my device to DMU systems?
No. There is no obligation for any member of staff to access university systems from their personal devices, however, many staff wish to do so. Staff are advised to ensure they fully understand the potential implications of connecting to DMU's systems before doing so.

Can I access DMU data via another means that gives me the access I need yet still protects me and the data?
Speak to the ITMS Service Desk on #6050 for advice. Webmail can be used to access your emails rather than setting up a mail account. Virtual Private Networks can be used with some systems to provide access to your files. This allows you to keep files on the University's systems where they are secure and backed up. Wherever possible, do not store DMU data on your personal device.

Why is the university so concerned about me connecting my device to their systems?
The university is required to adhere to the law and to contractual obligations in respect of data it holds. Legislation such as the Data Protection Act 1998, the Computer Misuse Act 1990 and the Privacy and Electronic Communications Regulations 2003, control what DMU is allowed to do with electronic information it holds, and it must take measures to ensure that breaches do not occur through allowing access to its data via mobile computing devices.

What should I consider before I connect my device to the university's systems?
If you are downloading and storing the university's personal data – that is data held by DMU that relates to living, identifiable human beings - on your device, the university has a legal obligation to ensure the security of that data. Other data may be subject to confidentiality contracts or business critical information.

Can the university wipe my personal device?
If your device connects directly to the DMU Microsoft Exchange system, there is the facility to wipe the device. If used, this functionality will wipe not only DMU owned data but all personal data, including contacts, text messages, accounts, etc, from that device. This functionality is a default part of the Exchange software. This functionality may be used by staff, for their own devices only, via the Webmail system and the ITMS email administration team (Unified Communications).

DMU will only ever wipe a device **with your written permission** or in exceptional circumstances (refer to section 4.3) or where it is impossible or impractical to obtain this and where it has been determined by the Chair of the Information Governance Board or their nominated deputy that it would be appropriate to protect confidential or personal data against unlawful access, such as in the event of the loss of your device. Once the functionality has been activated, the next time the device attempts to access the Exchange server, a command will be sent to the device to wipe it. For this reason it is important to securely back up your device on a regular basis.

Can the university access information stored on my device without my permission?

No. The only way the university can view or access any information on your device is **with your written permission** where you still have possession of the device. Be aware that in the event of a breach of the Data Protection Act, the Computer Misuse Act or other relevant legislation, a device holding university data could be removed by the police for investigation and may not be returned for some time. The access of DMU's networks or wifi is logged. Internet activity is logged.

How can I protect my device against loss, intrusion or harm?
Using old versions of software on any device can leave the device open to vulnerabilities and may cause loss, corruption or permit hackers to steal your data. Always ensure that your software is up to date. If it is available, you should run and keep updated antivirus software.

Disconnect from DMU systems and services as soon as you no longer require access to them.

Load applications such as 'Track my iPhone' or 'Google Device Manager' that allow you to remotely locate your device in the event of its loss. Only connect to wifi hotspots that you can trust.
Do not download untrusted or unverified applications to your device that may compromise your machine.

'Jail broken' devices, which is the process of removing limitations from the devices set by the manufacturers, should not be used to access DMU systems under any circumstances.

How do I configure my device to access DMU's systems?
Assistance is available on the Intranet here: https://sites.google.com/a/myapps.dmu.ac.uk/isas/help-support/self-help/mobile. Alternatively, contact the ITMS Service Desk on #6050.

What should I do in the event that my device is compromised (lost, stolen, infected by virus or corrupted)?

Contact your line manager as soon as possible and advise them of the issue.

You or your manager must contact the ITMS Service Desk (servicedesk@dmu.ac.uk 0116 2506050) as soon as possible to ensure that any compromise to DMU data can be minimised.

What should I do if I wish to give or sell my mobile device to a non-employee?

Employees must ensure that the device is permanently wiped of all DMU data and all links to DMU systems or services are permanently removed, such as email accounts, bookmarks etc. Contact the ITMS Service Desk on #6050 for further advice.

This version was last updated: 11th July 2016 by Neil Faver, IT Governance Manager ITMS