Mobile Computing Policy

1. Introduction

1.1. The purpose of this policy is to maintain the security of De Montfort (DMU) information assets when they are used from mobile devices or

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 equirements for information handling.

3.2. Should a member of staff elect to use a device not owned or managed by the university and the *Information Handling Policy* 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. F