Keele University Mobile Device Guidance

1. Introduction

1.1 Keele University is committed to preserving the **confidentiality**, **integrity** and **availability** of its data. Data once it is put on a portable device is immediately at greater risk of being compromised especially once the device is taken off site.

1.2 You are accountable for the security of the device and that data processed on it whilst it is assigned to you. Should the device be lost, stolen or the data on it is compromised, this will constitute a breach of the Data Protection Act 1998. In the event of a breach, you will have to demonstrate that your actions leading up to the theft, loss or compromise were reasonable.

1.3 Failure to comply with this guidance may constitute grounds for action under the University's disciplinary procedure.

2. Scope

2.1 This guidance applies to anyone who processes University data including staff, students, visitors and contractors. The guidance applies only to University provided mobile devices. For users who use their personal devices for University work there is separate Bring Your Own Device (BYOD) guidance that should be referred to. For the purposes of this guidance mobile devices include but are not limited to tablets (iPads etc), smartphones, laptops, video and audio recording equipment.

3. Requirements

3.1 **Do not** store University personal data on unencrypted mobile devices. If you are unsure if the device is encrypted you must contact the IT Service Desk. Personal data is any data that can identify an individual.

3.2 **Do not** store on unencrypted mobile devices any data that if it were compromised could have an adverse effect on the reputation of the University or the ability of the University to function.

3.3 **Do** only copy data to the mobile device when there is a legitimate and necessary need to do so. The device can be configured to use the VPN to connect to the Keele network so you can access data stored on the University network without the need to store it on the device. You should raise a support call with the IT Service Desk if you wish to have the device configured to use the VPN.

3.4 **Do not** copy personal data from the encrypted mobile device to a non-encrypted device or to a non-encrypted mobile device.

3.5 **Do** make sure that you back up the data on the mobile device to the University network drives and ensure that a unique copy is not solely stored on the device.

3.6 **Do not** access confidential information on the mobile device in locations where the contents of the device screen may be seen by non-authorised individuals.

3.7 **Do not** allow anyone else to use the University supplied mobile device including friends and family.

3.8 **Do not** leave the device unattended when travelling on public transport and keep it with you at all times. Store the device securely and out of sight when not in use.

3.9 **Do not** leave the mobile device unattended in a car.

3.10 **Do not** leave the mobile device unattended in insecure areas including your office if that is insecure. Make sure that the device is locked away in a secure location.

3.11 **Do not** write down the password/passcode to the device.

3.12 **Do** at all times abide by the contents of the IT Conditions of Use when using the mobile device.

3.13 **Do** report it immediately to the IT Service Desk and your line manager if the device is lost or stolen. You should also immediately change the passwords to all the University's services accessed from the device.

3.14 **Do** make sure that the software and anti-virus solution on the mobile device have the latest updates installed.

3.15 **Do** enable the PIN, password/passphrase feature on the device and make it as strong as the device will allow e.g. a 6 digits PIN instead of a 4 digits PIN or have a password/passphrase instead of a PIN.

3.16 **Do not** attempt to circumvent the device's security mechanisms e.g. "Jailbreak" the device.

3.17 **Do not** configure your device to automatically connect to available wireless access points. You must use your judgement about the security risk of connecting to a wireless network before doing so. You may have to account for your decision at a later date.

4. Contact

4.1 If you require further advice or you are in doubt about any of the contents of this guidance and what is expected of you raise a support call with the IT Service Desk or speak to your line manager. If you need advice about implementing any of the technical controls that are referred to in this guidance raise a support call with the IT Service Desk.