Keele University Bring Your Own Device Guidance

1. Introduction

1.1 Keele University is committed to preserving the **confidentiality**, **integrity** and **availability** of its data. The use of their own devices by employees for work purposes can be beneficial to the University but it also introduces new risks. The University does not have any control on the security mechanisms implemented on an employee’s personal device. If your personal device was lost or stolen there would be a risk that any University information stored on it could be accessed and exploited by unauthorised individuals.

1.2 You are accountable for the security of the University information whilst it is on your device. Should the University data held on your personal device be lost, stolen or the data is compromised, this will constitute a breach of the Data Protection Act 1998 and the loss will be investigated. As part of this investigation, you will be required to explain the steps taken to ensure the security of the data and the device.

1.3 The University reserves the right to refuse to allow access to particular devices or software where it considers that there is a security risk to its systems and infrastructure.

1.4 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 Keele employees who use their personal device to process University data. This is commonly known as “Bring Your Own Device” or BYOD. There is separate guidance for the use of Keele owned mobile devices. For the purposes of this guidance personal devices include but are not limited to home desktop PCs, tablets (iPads etc), smartphones, laptops, video and audio recording equipment.

3. Requirements

3.1 **Do** familiarise yourself with your device’s security features and ensure that the data processed on the device is afforded the maximum possible protection.

3.2 **Do** enable the PIN, password/passphrase feature on your device and make it as strong as your device will allow e.g. a 6 digits PIN instead of a 4 digits PIN or have a password/passphrase instead of a PIN. If there are biometric controls available they can be implemented. If you are unable to set a PIN or password on your device you **must not** process personal data on it. Personal data is any data that can identify an individual.

3.3 **Do** enable encryption on your device. If it is not possible to encrypt your device you **must not** store personal data on it or 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.

3.4 **Do** only copy data to your mobile device if there is a legitimate need to do so and only if there is no alternative. Once it is no longer necessary you must completely remove the data from your device including any email attachments containing data.

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

3.6 **Do** set your device to lock automatically after a small period of inactivity. The period of inactivity set should be no more than 2 minutes.

3.7 **Do** install and configure tracking services such as “Find my Phone” or “Where’s my Droid”.

3.8 **Do** configure your device so that in the event of it being lost or stolen it is possible to remote wipe its contents. If that is not possible you should set it to auto wipe the contents if the wrong PIN/password is entered ten times.

3.9 **Do** ensure that your device’s software is up to date and that it has the latest security patches installed.

3.10 **Do** install if it is available for your device anti-virus software and ensure that it is kept up to date.

3.11 **Do** ensure that other members of your household who may use your device cannot access University data.

3.12 **Do** completely remove all University information from your device once you cease to work for the University. This should be done by returning your device to manufacturer’s settings.

3.13 **Do** completely remove all University information from your device by returning it to the manufacturer’s settings before you sell, exchange or dispose of it.

3.14 **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.

3.15 **Do** exercise caution when downloading apps to your device. Malicious apps have been located in both the Google Play store and the Apple iTunes App store.

3.16 **Do not** attempt to circumvent your device’s security mechanisms e.g. “Jailbreak” the device.

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

3.18 **Do** abide by the contents of the IT Conditions of Use and other appropriate University Information Security policies and guidance including the University Mobile Device guidance when using your personal device for work purposes.

3.19 **Do** contact the IT Service Desk first before taking your personal device to an external organisation for repair if you use it to process University personal or confidential data.

4. Monitoring

4.1 The University will not monitor the content of your personal device but reserves the right to prevent access to the University's systems by any device that is considered a risk. The University also reserves the right to monitor and log data transferred between your device and the University's systems.

4.2 In exceptional circumstance it may be necessary for the University to access University data that is stored on your personal device. Every effort will be made to ensure that your personal data on the device will not be accessed.

5. Contact

5.1 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. Raise a support call with the IT Service Desk if you need advice about implementing any of the technical controls referred to in this guidance.