BYOD Policy: Use of Personally Owned Devices for University Work

University of Edinburgh Records Management

March 20, 2017

1 Audience and purpose

1.1

This policy is for all staff using personally owned devices such as smart phones, tablet computers, laptops, netbooks and similar equipment, to store, access, carry, transmit, receive or use University information or data, whether on an occasional or regular basis. The term for such devices is BYOD ("bring your own device").

1.2

The University recognises the benefits brought by the use of your own devices in work and welcomes it. This policy is about reducing the risk in using BYOD. Such risks may come from your BYOD being lost, stolen, used or exploited in such a way to take advantage of you or the University.

1.3

This policy sets out the minimum requirements. Individual business areas may specify additional, higher requirements as necessary.

```
'records-management' says BA can-say
  Device hasMet('higher-requirements')
  if Device isOwnedBy(Employee),
     Employee hasDepartment(BA).
```

1.4

We believe that following the procedures set out below will bring benefits to staff through protection of your own data as well as that of the University.

2 General principle

2.1

If you use your own device for University work, it is important to ensure that it and the information it contains is appropriately protected.

3 Data sensitivity

3.1

The Universitys Policy on Taking Sensitive Information and Personal Data Outside the Secure Computing Environment provides guidance on categories of high and medium risk personal data and business information.

3.2

If some of your work involves the use of high or medium risk information, and you use a BYOD, it is likely that some of it will find a way on to your device, for example within your email, or if you are working on documents away from your office.

4 Requirements for users of high and medium risk information; Advice for low risk users

4.1

High and medium risk users: You are required to comply with all bullet points listed below to permit use of BYOD for work. If necessary, seek help from your IT support personnel to meet these requirements.

```
'records-management' says Device hasMet('information-policy')
  if Employee has(Device),
     Employee hasMet('high-risk'),
     Device hasMet('high-risk-any-device-policy'),
     Device hasMet('high-risk-specific-device-policy').

'records-management' says Device hasMet('information-policy')
  if Employee has(Device),
     Employee hasMet('low-risk'),
     Device hasMet('low-risk-any-device-policy'),
     Device hasMet('low-risk-specific-device-policy').
```

4.2

Low risk users: For protection of your own data as well as low risk work data, you are advised to comply with at least the triangle bullet points below. Consider what the potential consequences could be for you, your friends or your family should your device become lost or stolen, and what protection configuration you want to put in place to prevent your data from being misused.

4.3

If you are in any doubt about which of the above classes you fall into you must assume that you are a High and medium risk user. Experience shows that almost all academic staff and those in HR, Finance and student-related roles will be high and medium risk users.

Any type of device

△ Set and use a passcode (e.g. pin number or password) to access your device. Whenever possible, use a strong passcode. Do not share the passcode with anyone.

△ Set your device to lock automatically when the device is inactive for more than a few minutes.

△ Take appropriate physical security measures. Do not leave your device unattended.

△ Keep your software up to date.

△ Make arrangements to back up your documents.

△ Keep master copies of work documents on a University managed storage service.

- If other members of your household use your device, ensure they cannot access University information, for example, with an additional account passcode. (Our preference is for you not to share the device with others.)
- Organise and regularly review the information on your device. Delete copies from your device when no longer needed.


```
'records-management' says Device hasMet('low-risk-any-device-policy')
  if Device hasPassword(Password),
     Password isStrongPassword,
     Device mustLockAfter(N),
     Device canBackupTo(Server),
     Server isOwnedBy('university')
  where leq(N, '180') = true.

'records-management' says Device hasMet('high-risk-any-device-policy')
  if Device hasMet('low-risk-any-device-policy'),
     Device isOwnedBy(Employee),
     Employee mustAcknowledged('erase-on-loss'),
     Employee hasAcknowledged('erase-on-loss'),
     Device isEncrypted.
```

- When you stop using your device (for example because you have replaced it) and when you leave the Universitys employment, securely delete all (non-published) University information from your device.
- Encrypt the device (to prevent access even if someone extracts the storage chips or disks and houses them in another device)[1][2].
- Report any data breaches in accordance with the Incident Reporting Policy.
- Configure your device to maximise its security. For example each new technology brings new enhanced security features. Take time to study and discover how to use these and decide which of them are relevant to you. Seek help from your IT support team if necessary.
- Whenever possible, use remote access facilities to access information on University systems. Log out and disconnect at the end of each session.

Mobile phones, smart phones and "tablet" devices

△ Configure your device to enable you to remote-wipe it should it become lost[3].

△ If your device is second hand, restore to factory settings before using it for the first time.

- Only download applications ('apps') or other software from reputable sources.

Laptops, computers and more sophisticated tablet devices

△ Use anti-virus software and keep it up to date

Using wireless networks outside the University

△ Control your devices connections by disabling automatic connection to open, unsecured Wi-Fi networks and make risk-conscious decisions before connecting.

△ Disable services such as Bluetooth and wireless if you are not using them.

[1]If your device is an Apple iPhone or iPad, it is encrypted and protection is effective as soon as you set a PIN locking code.

[2]If your device is Android, there is an option to turn on whole-device encryption in its configuration settings. Other devices may or may not be encryptable. We recommend that you include your ability to encrypt as a factor when you are choosing your own devices.

```
'records-management' says SmartPhone:Device hasMet('low-risk-specific-device-policy')
  if Device hasFeature('remote-wipe').

'records-management' says Device hasMet('high-risk-specific-device-policy')
  if Device hasMet('low-risk-specific-device-policy'),
     Device cannotSideload.
```

[3]If you configure your device for use with Office365, you are able to remote wipe it using a service within the university.

```
'records-management' says Computer:Device hasMet('low-risk-specific-device-policy')
  if Device has(Antivirus:AV)
  where update(AV) = true.
```

```
'records-management' says Device:D mustDisable('automatic-connection').
```

5 Consequences of non-compliance

5.1

The loss, theft or misuse of a BYOD is personally distressing. If you use sensitive data, it can also have serious consequences for others, for example staff and students about whom information is held. In addition there may be significant legal, financial and reputational consequences for the University, including fines of up to £500,000 can be levied. *You may also carry personal responsibility which, in serious cases could result in disciplinary action under the University Computing Regulations.*

```
'records-management' says Employee:U can-say
  U hasAcknowledged('compliance-policy').

'records-management' says Employee:U mustAcknowledged('compliance-policy').
```