IT Services

BRING YOUR OWN DEVICE POLICY

1. OVERVIEW AND PURPOSE

1.1. This document sets out the University's policy on the use of devices that are not owned or managed by the University to access University information and/or information technology services (commonly referred to as Bring your Own Device - BYOD) as part of the suite of Information Security policies.

1.2. Whilst the University recognises the benefits of allowing BYOD for work and study, such devices pose a security risk if not adequately protected.

1.3. The objective of this policy is to mitigate risks to the confidentiality, integrity and availability of University data, information and information technology services arising from BYOD.

1.4. This policy sets out the safeguards necessary to allow BYODs to access University information technology services without imposing unrealistic conditions on how such devices are configured.

2. SCOPE

2.1. This BYOD policy refers to any networked computing device with the capability to access the University's networked resources or services and that is not owned or managed by the University including, but not restricted to, phones, tablet computers, laptops, desktop

4.8.3. Users must take suitable precautions to protect the device and information being processed, including:

- Adherence to clear desk and clear screen practice
- Ensuring screens/sessions are locked or terminated when not in use
- Where possible, not leaving the device unattended
- Not permitting someone else to use the device whilst the University user session is unlocked

4.8.4. Users must follow the password policy, not divulge passwords to anybody and leave nothing on display that may contain information such as login names and passwords. Users should also avoid options such as "remember my password" or "stay logged in" on the device. The use of reputable password managers is acceptable.

4.8.5. Be mindful of information security if using devices during journeys in public environments to avoid the risk of theft of the device or unauthorised disclosure of University information by a third party observing the screen or keystrokes.

4.8.6. Users must take care when connecting to public networks, such as those provided by cafes and hotels, where there is an increased risk of interception. Appropriate care would be using a VPN to connect to University information technology services other than email, and ensuring an encrypted connection is used for email if not using VPN.

4.8.7. Users must report to IT Service Desk or on-site campus Security team any lost or stolen devices as soon as possible of becoming aware the device is missing, at least within 24 hours.

4.8.8. Notify any suspected breaches or weaknesses to the IT Service Desk.

4.8.9. Rooted (Android) and Jailbroken (iOS) devices are strictly forbidden from accessing the network.

4.8.10. No direct access to the Card Holder Data (CHD) environment is permitted from personally owned devices.

4.8.11. MAM-protected University information on the users' device will be remotely wiped if:

- The device is lost or stolen
- The device is no longer used, or access is no longer required
- On termination of employment / study / assignment (by either party)
- The device has been offline for more than 90 days
- A data or policy breach is detected
- A virus or similar threat to the security of the University's information technology services is detected.

4.8.12. Use of any non-University device is at the users' risk. In the unlikely event that a users' own data on the device is affected or lost, the University will not be held responsible or liable