MASSEY UNIVERSITY
TE KUNENGA KI PŪREHUROA
UNIVERSITY OF NEW ZEALAND

Massey University Policy Guide

MOBILE DEVICE POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	August 2016
Next Review	August 2019
Approval	SLT 16/08/163
Effective Date	August 2016

Purpose:

The purpose of this policy is to define the appropriate use of University supplied mobile devices by Massey University staff and authorised users, in order to:

- protect the integrity and confidentiality of institutional data that resides within Massey University's technology infrastructure
- prevent institutional data from being deliberately or inadvertently stored insecurely on a mobile device, or carried over an insecure network, where it can potentially be accessed by unsanctioned resources.

The objective being to reduce the risk of security breaches that could result in loss of information, damage to critical applications, or damage to Massey University's reputation.

Audience:

All users of Massey owned or supplied mobile devices must adhere to this policy.

Scope:

This policy covers mobile device access to Massey University data and the network. The term "mobile device" covered by this policy includes, but is not limited to, the following device types owned by the University:

- laptops and PCs with wireless networking capacity
- tablet computers (e.g. iPads)
- personal digital assistants (e.g. PDAs)
- mobile phones (e.g. smart phones, iPhones)
- Other smart devices (e.g. smart watches or wearable technology)
- portable storage (e.g. USB drives, portable hard drives, recordable media such as CDs and DVDs).

Policy:

Mobile Device Appropriate Use

- Mobile phones are issued for business purposes. Personal (non-work) related use of Massey-supplied mobile devices should be kept to a minimum. Where personal use incurs a cost against the device account, the device user may be required to reimburse the University for those costs.
- Premium Text Services, Text Shortcodes and Text Service Calls are not permitted on University-supplied mobile devices. Premium Text Services, Text Shortcodes and Text Services refers to a variety of services

that are available on mobile devices, and which generally result in additional ad hoc service charges against the mobile device account. Examples include, but are not limited to: Text to Park, ringtones, games, service alerts, competitions, charity donations, weather updates, subscription services and feedback or information on demand.

- Staff right of access and use of Massey University provided mobile devices and associated software ceases with termination of employment, and such equipment remains the property of the University.
- It is the responsibility of authorised mobile device users to ensure that all security protocols normally used in the management of data (on conventional storage infrastructure) are also applied when accessing or storing University resources on these devices.
- It is imperative that any mobile device that is used to conduct Massey business be used appropriately, responsibly and ethically.
- Users who operate mobile devices while working out of the office must also read and comply with the Remote Information Worker policy.
- Many mobile devices provide the user with ability to download, purchase, and run Applications (“Apps”) directly on them. Apps which are not permitted are those that breach the Internet Use and Digital Communications Policy, such as those containing objectionable material that may bring the University into disrepute, or are identified as creating an unacceptable information security risk.
- For all telecommunications enabled on Mobile devices, the Telecommunications Policy also applies.
- Unauthorised use of Massey mobile devices is prohibited.

Approved Mobile Devices

- Only ITS registered Massey mobile devices are authorised to connect to the internal University network. Prior to initial use on the University network, all Massey-owned mobile devices must be recorded and registered with ITS.
- Those devices not registered will only be permitted limited access to network facilities, to reduce the risk to information security.
- The Massey approved mobile devices list contains a set of approved mobile devices:
  - The most current and up to date list is available to all staff via the ITS published catalogue.
  - Devices not on this list must not be connected to the University network unless verified and approved by Massey ITS.
  - If your preferred device does not appear on this list, contact the Massey ITS Service Desk by phone on 06-356-9099 ext. 82111, or via the web, https://AskIT.massey.ac.nz.
- Massey owned and managed Windows or Mac operating system laptops and PCs will use the Massey Virtual Private Network (VPN) client when connecting to the University network while working remotely from the office.

Mobile Device Security

- All mobile devices must be protected by a password or key lock to prevent unauthorised use, which is required when a device is first turned on, and subsequently when left idle for not more than ten minutes.
- Passwords and key locks must not be written down, stored with the mobile device or disclosed to other persons. For further information, refer to the Usercode and Password Policy.
- Key locks must be treated in the same way you handle passwords, within the available limitations of the mobile device. They will be as unique and robust as possible and not contain birth dates, phone numbers or simple patters such as 1234, 1111, etc.
- All users of mobile devices must employ reasonable physical security measures to protect their mobile device when in use, when travelling with the device, or when it is unattended.
- Massey data stored on a mobile device must be cleared from the device when it is no longer required.
  - Regular reviews of data should be completed by the mobile device user, with all data identified as no longer required being deleted.
- IP routing must not be enabled on the mobile device:

  - Device-based IP routing presents a significant security risk when the mobile device is connected to two networks at the same time (e.g. a mobile device connected to a wireless access point while physically connected to the University network).
- No mobile device modifications to University hardware or software are to be made without the express approval of Massey ITS.
- The unauthorised use of mobile devices to back up, store and/or access sensitive University data containing personally identifiable information is prohibited.
- ITS undertakes wireless user and device access audit logging. Audit logs are reviewed and used to provide wireless activity reports on identify possible breaches and/or misuse that could jeopardise information security. Massey University reserves the right to use such logging and information to assist in investigations.

Reporting Mobile Device Loss and Security Issues

- In the event of a mobile device getting lost or stolen, the user must notify the Massey ITS Service Desk immediately by phone on on 06-356-9099 ext. 82111, for the following to be completed:
  - the remote device will be remotely wiped of all data and locked to prevent access to the device. Please note: This function is presently only available to certain types of mobile devices
  - the Massey domain user account passwords will be reset to eliminate the potential for unauthorised access to Massey public facing systems (e.g. Business Applications, VPN access, Web mail).
- All users must immediately report to their manager and the Massey ITS Service Desk any incident, or suspected incidents, of unauthorised data access, data loss and/or disclosure of company resources, databases, networks etc.

Definitions:

Conventional Storage Infrastructure

The data storage technology employed at Massey University premises to store, manage and protect data and information. This could be mapped network drives, staff intranet website, or information stored in an application that is only available to authorised staff.

Information Security

Directly relates to providing for the confidentiality, integrity and availability of all digital resources within Massey University. This provides assurance that information is only accessible by those who are authorised to view it, records and data are valid and correct, and mission critical information is accessible when it is needed.

Key locks

In this document used as a term to describe screen saver passwords or other similar security mechanisms on mobile devices that require the device to be unlocked each time it is switched on or left idle for a period of time. This prevents unauthorised users from using the device.

Malware

Programming code, scripts, active content, and other software designed to disrupt, collet private information, or gain unauthorised access to system resources.

Network facilities

Information Communication and Technology systems accessed via connection to the University network, which includes, but is not limited to, email, printing, teaching spaces, internet and world wide web.

Personally Identifiable Information

Data contained in University systems that is private information, as defined by the Privacy Act.

Firewall

A security application running on a device designed to protect and control network traffic to and from the device.

VPN

Or Virtual Private Network is a secure and encrypted connection between a remote client device and the internal Massey network. It acts to secure data transmitted over a typically insecure network (such as the internet) to a corporate (private) network.

Legal compliance:

Nil

Related policy and procedure compliance:

Endpoint Device Policy
Remote Information Worker Policy
Telecommunications Policy
Internet Use and Digital Communications Policy
Usercode and Password Policy

Related procedures / documents:

ISO/IEC 27000:2014 – Information technology – Information security management systems
Massey University Information Security Manual
Information Security @ Massey

Document Management Control:

Prepared by:	Information Technology Services
Authorised by:	The Chief Information Officer
Approved by:	SLT 16/08/163
Date issued:	August 2016
Last review:	August 2016
Next review:	August 2019