MOBILE DEVICE MANAGEMENT POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	November 2020
Next Review	November 2023
Approval	SLT 21/02/17

Purpose:

The purpose of this policy is to define standards, procedures, and restrictions for users who have a legitimate business need for connecting mobile devices to Massey University's corporate network and data.

Key success factors:

- Confidential data that resides within Massey University's technology infrastructure, including internal and external cloud sources, is protected
- Data is protected from being deliberately or inadvertently stored insecurely, on a mobile device, or carried over an insecure network where it could potentially be accessed by unsanctioned resources
- Centralised management of all mobile devices is owned by the University.

Audience:

All users or anyone using the Massey network via a mobile device whilst working on behalf of the University. Users include Massey University staff and students (including but not limited to contractors, consultants and volunteers).

Policy:

This mobile device policy applies, but is not limited to, all devices and accompanying media that fit the following:

- smartphones
- other mobile/cellular phones
- tablets
- e-readers
- portable media devices
- portable gaming devices
- laptop/notebook/ultrabook computers
- wearable computing devices
- personal digital assistants (e.g. PDAs)
- any other mobile device capable of storing corporate data and connecting to a network.

The policy addresses a range of threats to University data, or related to its use, such as:

Threat	Description
Device Loss	Devices used to transfer or transport work files that could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, worms, spyware, malware, and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the University to the risk of non-compliance with various identity theft and privacy laws.

Policy Statements:

1. The **Vice-Chancellor** has overall responsibility for the confidentiality, integrity, and availability of corporate data.

2. The **Chief Information Officer** has delegated execution and maintenance of information technology and information systems.

3. All users or anyone using the Massey network via a mobile device whilst working on behalf of the University are responsible to act in accordance with University policies and procedures. Users include Massey University staff and students (including but not limited to contractors, consultants and volunteers).

4. Connectivity of all mobile devices will be centrally managed by the ITS department and will use authentication and strong encryption measures. Although ITS will not directly manage personal devices purchased by employees, ITS will apply minimal controls to protect University information when used on a personal device. End users are expected to adhere to the same security protocols when connected to the Massey network. Failure to do so will result in immediate suspension of all network access privIleges so as to protect the University's infrastructure.

Mobile Device Appropriate Use

Massey-supplied mobile devices

1. Massey-supplied mobile devices 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.

2. Premium Text Services, Text short codes and Text Service Calls are not permitted on Massey-supplied mobile devices.

3. Staff right of access and use of Massey supplied mobile devices, and associated software, ceases with the termination of employment, and such equipment remains the property of the University.

4. All users that are in possession of a Massey-supplied mobile device must ensure that the usage of calls and text messages remains within the quota of their allocated plan.

5. Massey mobile connections are given a limited allocation of mobile data per month. If usage regularly or excessively exceeds this amount, ITS may contact the user's financial administrator to discuss additional costs being met by their department. Repeat excessive use may result in a user's data connection being disabled.

6. Many mobile devices provide the user with the ability to download, purchase, and run Applications ("Apps") directly on them. Apps which are not permitted are those containing objectionable material that may bring the University into disrepute or are identified as creating an unacceptable information security risk.

All mobile devices

7. It is imperative that any mobile device that is used to access Massey information is secure.

8. For all telecommunications enabled on mobile devices, the Telecommunications Policy also applies.

Mobile Device Management (MDM)

Massey-supplied mobile devices

1. ITS uses a mobile device management solution to secure devices and enforce policies remotely. Before connecting a mobile device to corporate resources, the device will be automatically enrolled prior to being issued to the user.

2. The vendor's device management solution must be installed on any Massey-supplied mobile device.

3. The mobile device management solution enables ITS to take the following actions on Massey-supplied mobile devices:

    - remote wipe of Massey owned information. Personal information will not be affected
    - enforcement of security policies, including mandating the use of a PIN to secure the device
    - location tracking if the device is lost or stolen
    - application deployment and visibility
    - hardware feature management.

Personally owned mobile devices

4. ITS uses a mobile device management solution to secure devices and enforce policies remotely. Before connecting a mobile device to Massey corporate resources, the device must be recorded and registered with ITS.

5. The mobile device management solution enables ITS to take the following actions on personally owned mobile devices:

    - remote wipe of Massey owned information. Personal information will not be affected
    - enforcement of security policies, including mandating the use of a PIN to secure the device.

All mobile devices

6. Any attempt to contravene or bypass the mobile device management implementation may result in immediate disconnection from corporate resources.

Approved Mobile Devices

Massey-supplied mobile devices

1. All Massey-supplied mobile devices must be procured from an authorised supplier via the University's purchasing system through ITS:

    - the most current and up-to-date mobile handset list is available to all staff via the mobile phones page on the ITS intranet; other devices are available via the ITS published catalogue
    - devices not on the 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.

2. All University procured mobile devices must be used in conjunction with a Massey University mobile plan.

3. All mobile devices that are the property of Massey University must be returned to ITS upon upgrade or termination of employment.

All mobile devices

4. Prior to intial use on the University network, all mobile devices must be recorded and registered with ITS.

Mobile Device Security

All mobile devices

1. All mobile devices must be protected by a strong password or pin code to prevent unauthorised use.

2. Passwords and pin codes must not be written down, stored with the mobile device or disclosed to other persons. For further information, refer to the Password Policy.

3. 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.

4. 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.

5. No mobile device modifications to University issued hardware or software are to be made without the express approval of ITS.

6. The unauthorised use of mobile devices to back up, store and/or access sensitive University data containing personally identifiable information is prohibited.

7. ITS undertakes wireless user and device access audit logging. Audit logs are reviewed and used to provide wireless activity reports to 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.

8. In the event a mobile device is lost or stolen, the user must notify the Massey ITS Service Desk immediately.

Definitions:

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.

Malware means programming code, scripts, active content, and other software designed to disrupt, collect private information, or gain unauthorised access to system resources.

Network facilities are Information Communication and Technology (ICT) 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 means data contained in University systems that is private information, as defined by the Privacy Act.

Premium Text Services, Text short codes 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.

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.

Relevant Legislation:

Related policy and procedures:

Acceptable Use Policy
Desktop Hardware and Software Policy
Device Security Policy
Intellectual Property Policy
Official Information Act
Password Policy
Policy on Staff Conduct
Student Academic Integrity Policy
Telecommunications Policy
Service plans and mobile data

Document Management Control:

Prepared by: Chief Information Officer
Authorised by: Deputy Vice-Chancellor, Finance and Technology
Approved by: SLT 21/02/17
Date issued: August 2016
Last review: November 2020
Next review: November 2023