Griffith UNIVERSITY

MS Intune Terms and Conditions

These terms and conditions apply to all employees, contractors, students, volunteers and consultants of Griffith University who use MS Intune to access Griffith University data & applications on their mobile devices. By accessing Griffith University data & applications on your mobile device through MS Intune you agree to comply with these terms and conditions. If you do not agree to these terms and conditions, do not access Griffith University data & applications on mobile devices through MS Intune. There may be serious consequences for non-compliance with this standard, including disciplinary action.

1. Statement

MS Intune (the Service) provides authorised users with access to Griffith University Office of Digital Solutions (ODS) systems on their corporate issued and/or BYO device while protecting the confidentiality, privacy, integrity, security and availability of Griffith University data and systems.

There are two use cases the Service. The first of these is where the University issues a device to an employee (corporately-owned device) and the second is where an employee brings their own device and uses this to access University information (BYO).

2. Scope

These terms and conditions apply to both corporate issued and BYO devices.

Devices running the following operating systems are able to use MS Intune:

- iOS
- Android
- Windows 10 (BYOD only)

3. Terms of Use

Use of the Service, whether or not on corporate or BYO devices shall be subject to all relevant Griffith University Policies including the Information Technology Code of Practice and the Information Security Policy.

Accessing the Service shall not affect conditions of employment or, of itself, accrue to the authorised user any related benefits or privileges not otherwise able to be accrued by the user.

4. Requirements

Prior to enrolling

Prior to enrolment in, and during the use of the Service, the user must ensure that:

1. The operating system on the device is up to date and in the form intended by the manufacturer;
2. Malware is not installed on the device;
3. Personal data or information on the device has been copied to a secure backup location if the authorised user seeks to retain the information; and
4. Their personal details recorded in their Griffith University employment records are current and up to date.

Security setup on device

Implementing the following security settings is a requirement of enrolling and using the Service:

1. The user must set a security code of 4 characters or touch-points (passcode, password, touch-point pattern or backup access password or fingerprint ID) on the device as a pre-requisite to accessing and using the Service. The user must also set the device so a maximum of 10 consecutive incorrect access attempts permitted before access to the device is suspended for an incremental time period base on further failed attempts;
2. The Authorised User must set device to lock after 5 minutes of inactivity; and
3. The User must contact the Griffith University IT Service Centre on 3735 5555 as soon as possible:
    a. If the device is lost or stolen; or
    b. Upon becoming aware that the security or privacy of Griffith University Information stored through the Service on the device may have been compromised; or
    c. If the device has been replaced.

The user must notify the IT Service Centre on 3735 5555 forthwith upon no longer working for, engaged with or a student of Griffith University.

5. Griffith University's Rights

By accessing and using the Service, the user acknowledges that Griffith University may:

- Through its Office of Digital Solutions, maintain a list of all the packaged applications which support the Service and which are delivered to devices and monitor the security settings of those applications and devices;
- Periodically collect the device location if the user allows Location Services during the user's enrolment with the service;
- Erase all data stored on the device through the Service where a staff member's working, consultancy, student, contract or volunteering relationship with Griffith University is no longer current, if the relevant device is reported lost or stolen or otherwise in response to an actual or potential security threat. Griffith University accepts no responsibility for personal data erased from a user's device if that data has been stored using the Service; and
- If a device has not accessed the Service for 90 calendar days Griffith University may automatically disenroll the device from the Service and erase all data stored on the device through the Service.

6. Your Obligations

Each user agrees to comply with the following conditions of use as a requirement of enrolling in and using the Service:

1. Keep the security code on the device secret and not disclose it to any other person;
2. Keep the device compliant with all of the security settings set out above;
3. Not modify or attempt to modify the configuration of Service application on the device or attempt to circumvent any security measures implemented as part of the Service or install malware; and
4. When connected to the Griffith University network:
   a. Not allow any other person to access Griffith University Information using the BYO device;
   b. Not leave the device connected or unattended without adequate security code protection;
   c. Ensure that all Griffith University content is viewable only in an environment where the content cannot be observed or heard by persons who are not authorised to access the information; and
   d. Not misuse any Griffith University content – for example by using screen capture tools or unauthorised disclosure or copying.

All personal information collected through the Service will be dealt with by Griffith in accordance with these terms and conditions and the University's Privacy Plan

7. Responsibility and Liability

- The User is solely responsible for backing-up the User's personal information on the device. This includes personal information like photos and personal contacts. Griffith University assumes no responsibility for the loss of personal data stored on your device.
- The User is responsible for all carrier and other costs associated with the use of a BYO device and acknowledges that Griffith University shall not be liable for any loss, including any costs, or damage directly or indirectly related to the BYO device or any other personal hardware, software or information of the authorised user or any other person, or any performance degradation, diminished functionality or inconvenience.
- The user indemnifies Griffith University for any loss or damage to the extent it results from the user's use of the Service other than in compliance with this user agreement.
- It is the user's responsibility to contact vendors for trouble-shooting and support of third-party software and the user acknowledges there is limited configuration support and advice provided by the Office of Digital Solutions.
- I understand that my personal information provided to the Griffith University to facilitate administration in relation to, maintenance of, and my access to MS Intune will be dealt with by Griffith University in accordance with its privacy plan which is available at https://www.griffith.edu.au/about-griffith/corporate-governance/plans-publications/griffith-university-privacy-plan.

Prepared by: [Student Digital Workspace project team]
Last modified: [26/06/18]