MCD Data Push Terms of Service

University employees are eligible to connect to the university email/calendaring system via "data push" to a mobile computing device (MCD) for business purposes. This Terms of Service document outlines the responsibilities and guidelines for appropriate use of the data push service, whether from a university-owned or privately-owned device. To minimize risk in the event of theft or loss of mobile devices, it is very important that your device enables reasonable security features including:

1. Require passcode re-entry after a period of inactivity
2. Require a reasonable passcode to unlock your device (i.e. not 1111)
3. Require annual passcode change
4. Require use of built-in device encryption
5. Require device to be self-erased in the event of too many incorrect password attempts
6. Allow remote wiping of the device if it is lost or stolen

The above settings are mandatory and are pushed to devices when they are registered for this service. This enhances security of access to university mail, calendar, and contact information on mobile devices and protects your information from abuse by unknown and unauthorized persons.

University Rights and Responsibilities

- The university will push security policies onto registered devices to safeguard the institution and its information assets. If a device is reported as lost, or stolen, or when an employee is terminated or otherwise ineligible, the university whenever possible will remotely remove university data/email only, otherwise the device will be remotely “wiped” and set back to factory defaults.
- WCU IT staff will provide “best effort” support to initial setup only. For other configuration troubleshooting for your device, you are required to contact your service provider.
- In the event an employee is terminated or is otherwise ineligible for data/email access, the employee’s account and access to the data push service will be discontinued.

Employee Responsibility

- Employees are required to notify the IT Help Desk within 24 hours of the loss or theft of their device.
- If theft is suspected, employees must file a police report and cooperate with law enforcement to ensure the institution’s interest in preserving confidential information is respected.

Appropriate Use

All MCDs that access University resources are subject to the Mobile Computing Devices Standard operating under University Policy 117 Information Security. In addition, **users of the data push service will not attempt to modify or bypass the security settings (such as jailbreaking)** that WCU IT pushes to your device.

Terms of Service Non-Compliance

Failure to comply with the MCD Data Push Terms of Service may result in suspension of access privileges to university data/Email.

Employee Declaration

Continuing to use the University’s data push service implies the following:

- I have read and understand the above MCD Data Push Terms of Service and consent to adhere to the rules outline therein. Furthermore, I agree that the university reserves the right to install and push security policies onto my device as needed without prior notification in order to safeguard the institution and its informational assets.