Policy: Acceptable Use of Mobile Devices

Version and approval

Effective Date:	August 21, 2018
Last Updated:	August 9, 2018
Approved by:	Dave Robinson, Chief Information Officer

Purpose

The purpose of this policy is to protect Grinnell College data on Mobile Devices. This policy defines the standards, procedures, and restrictions required of Mobile Devices to help ensure the security of Grinnell College data and networks.

Review cycle

The Director of Information Security shall annually review this policy.

Scope

This policy applies to all handheld and wearable devices and tablets that store or access Grinnell College data (“Mobile Devices”).

Policy Owner

The Policy Owner is the Director of Information Security, Information Technology Services (ITS).

The Policy Owner, or the Chief Information Officer, is responsible for interpreting this policy.

Related Policies

All other relevant policies, including the Academic Computer Usage Policy, must be observed when using Mobile Devices.

Access Control

ITS reserves the right to limit or refuse, by physical and non-physical means, the ability to connect Mobile Devices to Grinnell College and Grinnell College-connected infrastructure. ITS may engage in such action if Mobile Devices are used in a way that is not in accordance with this policy or puts the College, its systems, data, or users at risk or potential risk.

Security

A strong passcode or PIN (“Passcode/PIN”) must protect all Mobile Devices. All data stored on the device must be encrypted using strong encryption. Users with Grinnell College credentials agree never to disclose their Passcode/PIN to anyone.

Users are expected to secure Mobile Devices at all times using reasonable physical security measures.

Data categorized as “Restricted” or “Internal” (as described in the current edition of the Grinnell College Data Classification Guide) are not to be stored unencrypted on Mobile Devices. Grinnell College data stored on mobile devices should be kept to a minimum. Data must be immediately and permanently deleted using Grinnell College-sanctioned data removal procedures once there is no legitimate reason to retain the data.

ITS may centrally manage security policies, network, application, and data access utilizing technology solutions assessed to be appropriate by the Director of Information Security. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt.

In the event of a lost or stolen Mobile Device, the User must report the incident to the ITS Technology Services Desk immediately. Where possible, Grinnell College data (including email) stored on the Mobile Device will be remotely wiped by authorized ITS personnel. The remote wipe may destroy all data on the Mobile Device. Connecting to the Grinnell College email server requires Users to allow remote wipe functions.

Users agree to report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of Grinnell College data to the ITS Technology Services Desk immediately.

Mobile Devices must meet the following minimum security settings:

- Passcode/PIN required to unlock Mobile Devices
- Length of Passcode/PIN: 6 characters
- Passcode/PIN to be changed a maximum of every 180 days
- Passcode/PIN is required after 5 minutes of inactivity
- Do not reuse any of the last 10 previous Passcodes/PINs
- Factory reset after a maximum of 15 incorrect access attempts

Biometrics are permissible if a compliant Passcode/PIN is required before the Mobile Device starts up.

Cellular Mobile Devices must meet the following minimum operating system version:

- iOS version 9 and above
- Android version 5.1.1 and above

Users will make no modifications to the hardware or software of the Mobile Device (e.g., replacing or overriding the operating system, jailbreaking, rooting)

Mobile Device Lifecycle

Any Mobile Device that has accessed or stored Grinnell College data must be completely and securely wiped prior to ownership change, disposal, or recycling. ITS is available to assist with the secure wipe process.

Resources

Help documentation is available online for assistance with the configuration of Mobile Device security settings.

The Technology Services Desk team of professional staff and students is available to help troubleshoot and fix a wide range of technology questions. The Technology Services Desk is open weekdays between 8am and 5pm. You can stop by the Forum (upper level, south), phone (641) 269-4901 (x4901), or email TechnologyServicesDesk@help.grinnell.edu for support. After-hours support is available by phone.