Mobile Device Management (MDM) Privacy Information

We respect your privacy. MobileIron MDM cannot access your application data, call history, voicemail, or SMS (text) messages on your mobile device. We cannot and do not collect your personal data nor GPS location information. Please use this sheet as a reference for the information we collect and why.

INFORMATION WE COLLECT

- **Device ID and data on storage capacity, operating system, carrier, and firmware** – *to uniquely identify devices and ensure correct records in the event a device is lost or stolen*
- **MDM installed apps** – *does not include personal apps*
- **Jailbreak or root detection** – *to determine if built-in security features were bypassed or disabled*

The comprehensive list of information collected for each device can be found below:

- Name
- UDID (unique device identification)
- WiFi MAC address
- Phone number
- Cellular technology
- Cellular network ID
- Model number
- Model name
- SIM Carrier
- Device serial number
- Carrier settings version
- Capacity
- Jailbreak or root status
- Time of enrollment
- Time of MobileIron access

For your awareness, below indicates the CUIMC's MobileIron default privacy settings:

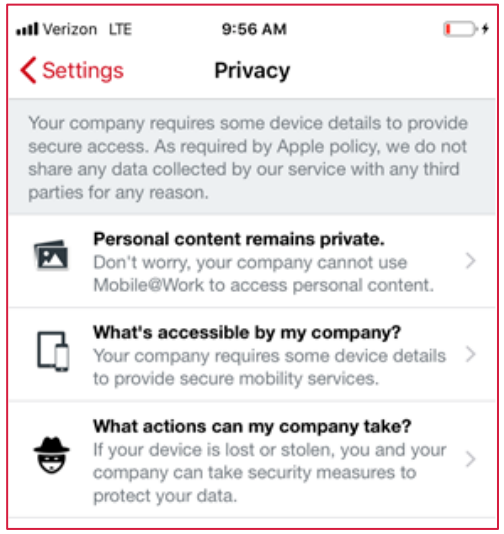
CUIMC MobileIron Privacy Settings	
Setting	**Status**
Configuration Profiles	Enabled
Call Logs	Disabled
SMS Logs	Disabled
Sync Location	Disabled
Android Warning Banner on Device Reboot	Disabled
Apps	App Catalog Apps

MDM Privacy Configuration

Our policies allow the Information Security Office to **monitor University systems, data, and networks but not personal**. Device information is available for corporate issued phones for lost or stolen university property.

Location tracking for MobileIron is available through an end-user setting on the device which can be turned on or off.

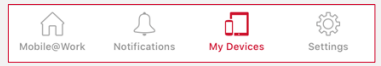
BYOD devices* are automatically opted-out of the MDM location feature. Thus, Columbia will not be able to provide any information regarding the device's last known location in the event the device is lost or stolen. **Personal devices will not be able to join the university network nor interact with university assets.**



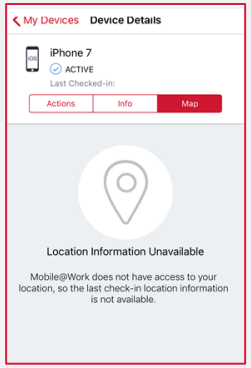
Users are not required to install MDM or access Epic on personal devices. The only requirement is to have a mobile device to access Epic. If preferred, users can provision a separate device for university work.

To view your current configuration, follow these steps:

1. Open the MobileIron application on your device
2. Select the "My Device" tab located at the base of the app page



3. If prompted, log in with your CWID username and password credential
4. Select your device and click on the tab "Map" to verify location information is unavailable via Mobile@Work



5. For additional information on your device's "General Setup", select the settings option to view details