CHAPMAN UNIVERSITY | Information Systems and Technology

Mobile Computing Device Standard

Table of Contents

1.0 PURPOSE:

The intent of this standard is to describe Chapman University's methodology for ensuring appropriate safeguards for the use and security of mobile computing and storage devices both in campus facilities and off campus as referenced in *Chapman University Computer and Network acceptable use policy.*

2.0 DEFINITIONS:

Sensitive Computing Devices: Magnetic Stripe Readers, Wireless Access Points, Handheld credit card devices, Smartphones, Tablets

3.0 BACKGROUND:

Mobile Devices may be provided and owned by Chapman or may be owned by the employee.

This standard is intended to protect the security and integrity of Chapman's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Chapman University must have a process for monitoring and distributing sensitive mobile computing and storage devices which may have impacts on important data.

Chapman staff and faculty must agree to the mobile device standard in order to connect their devices to the University network. Continued use of corporate cellular or BYOD services constitutes agreement with this standard.

4.0 REQUIRED MATERIALS AND SUPPLIES TO EXECUTE PROCEDURE:

Cell Phone Receipt Acknowledgement - Form Appendix B

5.0 ROLES AND RESPONSIBILITIES for CU owned device:

5.1 Operation of Appropriate Use

Users must comply, including but not limited to, the following:

a) Devices must be used in a manner that complies with Chapman University's Computer and Network Acceptable Use Policy and Harassment, Discrimination, and Sexual Harassment Policy.
b) Access to data of certain risk classifications or access to a 3rd party dataset through a Chapman University agreement may require additional requirements and safeguards. Also, User is explicitly prohibited to download any Chapman University Content data

that is classified HIGH Risk as outlined in Chapman University's Data Risk Classification website.

c) Chapman University prohibits User from using Devices in an illegal manner while operating Chapman vehicles, machinery, or equipment. User must also comply with Chapman University's Transportation Policy.
d) User is responsible for complying with applicable Chapman University export control guidelines when performing University related work on personal devices outside the US.
e) Employees must safeguard mobile computing and storage devices and any sensitive data stored/transmitted by them with the same protections afforded hardcopy sensitive documents of Chapman University.

5.2 Operation of Chapman University Computing and Storage Devices

a) Mobile computing and storage devices should be treated as any other Chapman University-owned equipment, used only by employees or student workers to execute work-related tasks as approved by management.
b) Employee shall not remove or alter any identification labels that are attached to or displayed.
c) Alterations of hardware are prohibited. Jailbroken or rooted devices are strictly forbidden from accessing the network. If a provisioned device is found in this condition its access will be revoked immediately.
d) Should additions be made to the device, such amenities will become the property of Chapman University. IS&T is not responsible for maintenance of or providing technical assistance for any non-standard applications or reconfigured hardware.
e) Chapman University documents information concerning checking out and tracking of mobile computing and specified storage devices.

5.3 Chapman University's Rights to Data

a) In order to prevent misuse and to protect Chapman University's data, **Chapman University reserves the rights to monitor, review, make copies, preserve, and *Sanitize*, without further notice, all data including personal data, that is within *Chapman University Content* on *the Device*, at Chapman University's sole discretion.**
b) Although Chapman University does not make a practice of monitoring non-Chapman University data transferred over Chapman University's network. **Chapman University may monitor, review, make copies, preserve any data transmitted over Chapman University's network, including personal data, for litigation, investigations, as otherwise required by law.**
c) Chapman University may also require to obtain *the Devices*, and other data relating to Chapman University from *the Devices*, **which may include *User's* personal data** for litigation, investigations, as otherwise required by law, and in accordance with Chapman University's Privacy Policy.

d) IST will gather and maintain the below information on Chapman mobile devices:
    i. Employee who will be using the device; Management approval; Item description and intended use; location, serial number, asset tag, make and model numbers.

5.4 Security

Devices will be monitored for compliance to configuration policies, installed software, software version and patch levels, and other security-related items. Employees have no expectation of privacy with respect to use of the device while it is CU-managed and has access to CU information.

a) In order to prevent unauthorized access, devices must be password protected using the features of the device.
b) The device must lock itself with a password or personal identification number (PIN) if it's idle for five minutes or less.
c) After ten failed login attempts, the device will be erased.
d) Encryption is required to be enabled on the device
e) Employees' access to company data is limited based on user profiles defined by Information Security and automatically enforced.

5.5 Condition for Chapman University's Right to *Sanitize* Data

Any data on *the Devices* may be *Sanitized* or disconnected from access to Chapman University's network by Chapman University including but not limited to:

a) if the *Devices* are lost, stolen, or no longer will be used for Chapman University's business or on behalf of Chapman University;
b) if the *User's* relationship with Chapman University ends; or
c) if Chapman University detects a data or Policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

5.6 Acceptable Environmental Conditions for Use of Mobile Computing or Storage Devices Outside Campus Facilities.

a) The mobile computing or storage device may not be left unattended in public areas.
b) When located within a campus facility, university owned mobile computing devices must be stored in locked file drawers, locked rooms, closets or cupboards, or locked down to the desktop.
c) Guidelines on reporting loss or theft of Chapman University property, including sensitive computing devices, are provided in *Property Loss or Theft of Information Assets - Procedure.*

6.0 Personal owned devices: user responsibility procedures

Please refer CU BYOD policy for more details

APPENDIX A: REFERENCES

BYOD policy (approved pending full return to in person instruction)

APPENDIX B: Chapman Cell Phone Receipt Acknowledgement

1. By signing this acknowledgment, you agree to immediately report any theft or loss of the phone to Network Services and your supervisor. To safeguard against actual or threatened compromise of the CU's information, you consent to the CU deleting all information on the phone, including all personal, non-CU related data or information, if the phone is lost, stolen or if any other situation occurs where the CU – in its sole discretion – believes that the confidentiality of CU information has become jeopardized.

2. You understand that the use of the phone is subject to and governed by the CU's Communication Systems Policy. You acknowledge that you have no right to privacy with respect to the use of the phone. You acknowledge that CU can review any data or information stored in, created with, received by, or sent over the phone for any legitimate business reason at any time. You acknowledge that the CU's Information Security department will manage and monitor security settings and installed software on the phone at any time.

3. The CU's monthly phone service plan ("plan") includes the following: (can make appendix)

    - E.g. Shared Pool of anytime minutes
    - Free domestic calls between 9:00pm – 6:00am Monday through Friday
    - Free domestic calls Saturday and Sunday
    - Free Mobile to Mobile among Verizon customers
    - PDA Devices have 2 GB of data
    - 200 Text Messages (additional texts are $.20 per message)

4. You understand that you may use the phone for personal calls. However, you will be responsible for reimbursing the CU for any and all charges accrued due to unauthorized overages, including but not limited to, international fees, roaming, text, or download fees. You authorize the CU to deduct any such unauthorized charges from your paycheck.

5. If you elect to receive a Chapman-provided phone, you agree that the phone, phone number, and plan belong to CU. If your employment with the CU terminates, the phone's service will be canceled and all data and information, whether CU-related or personal, will be deleted immediately from the phone. Upon termination of your employment, you will return the phone to the CU immediately. Should you fail to return the phone to the CU, you authorize the CU to deduct the purchase price of the phone from your final paycheck.

6. If you elect to purchase an upgraded phone, you agree that the phone number and plan belong to the CU. If your employment with the CU terminates, the phone's service will be canceled and all data and information, whether CU-related or personal, will be deleted immediately from the phone.

7. You understand it is your responsibility to back-up any personal data you may add to the phone.

I acknowledge that I have read and understand the above conditions.

Employee Signature:

_____Date:_____

Please Print Name:

_____