California Western School of Law
Mobile Device Policy
Updated July 2014

1.0 Overview

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. *The user community is strongly encouraged to access data via a remote connection to your desktop, that is, you can access your desktop from anywhere. It is simple to use this secure connection and IT can instruct you. Users may use cloud solutions to sync files to all devices and therefore consideration must be given to the security of mobile devices.*

2.0 Purpose

The purpose of this policy is to specify school standards for the use and security of mobile devices.

3.0 Scope

This policy applies to school data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with school data.

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The school and its employees must carefully consider the physical security of mobile devices and take appropriate protective measures, including the following:

- Laptop should be secured in drawers and/or kept out of site when in the office or other fixed locations.

- Mobile devices should be kept out of sight when not in use.

- Care should be given when using or transporting mobile devices in busy areas.

- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

- CWSL will evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable

- The CWSL will continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting school data. The following sections specify the school's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

Use of encryption is not required but it is encouraged if data stored on the device is especially sensitive. Laptops need to be secured with a username and password or biometrics for login.

4.2.2 PDAs/Smart Phones

Use of encryption is not required on PDAs/smart phones but it is encouraged if data stored on the device is especially sensitive. PDAs/smart phones must require a password for login.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of school data on such devices is discouraged; their use is permitted only when necessary and encryption is not required.

4.2.4 Portable Media Players

No school data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing school data on other mobile devices, or connecting such devices to school systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the Executive Director of IT.

4.3 Connecting to Unsecured Networks

Users are permitted to connect school-provided computers to public or unsecured networks. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the school. It is prohibited to network.

4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a mobile device must be reported promptly to the Executive Director of IT and/or the Cabinet.

- Confidential data must not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured, password protected and comply with the Confidential Data policy.

- Data stored on mobile devices must be securely removed and unrecoverable in accordance with the Data Classification Policy upon termination of employment or when data is no longer needed. Information Technology can help to ensure all data is wiped.

4.5 Applicability of Other Policies

This document is part of the school's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Executive Director of IT and/or the Cabinet. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of school property (physical or intellectual) are suspected, the school may report such activities to the applicable authorities.

6.0 Definitions

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media A data storage device that utilizes flash memory to store data. These devices are often called a USB drive, flash drive, or thumb drive.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA Stands for Personal Digital Assistant. This is a portable device stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.