Mobile Device Usage Policy

The state recognizes mobile devices for many personnel are valuable tools that aid the state in conducting business in an effective and timely manner. These tools can help employee productivity and promote public and employee safety. This policy intends to address privacy and related issues raised by mobile device usage.

# PURPOSE

This Policy defines the minimum steps expected of state agencies in order to ensure the efficient assignment, use and management of mobile devices while protecting employee privacy, client privacy and consumer information. This policy is intended to:

* Enhance the security of state operations and information assets;
* Ensure agencies and employees are aware of their responsibilities; and
* Clarify employees’ expectation of privacy in communications on both state-issued and personal devices.

# POLICY STATEMENT

1. Agencies must determine which of three categories of devices their employees may use on the job:
	1. State-Owned Devices;
	2. Personal Devices with state Mobile Device Management (MDM) or Enterprise Mobility Management (EMM);
	3. Personal Devices with no state management software.
2. Agencies must adopt a Mobile Device Policy and directly communicate that policy individually to each of their employees on an ongoing basis as policies evolve.
3. Agency Mobile Device Policies must:
	1. Govern employee use of mobile devices on the job;
	2. Articulate employees’ basic rights and responsibilities concerning mobile device usage;
	3. Ensure that the agency receives access to public records produced or stored on mobile devices, including encrypted communications;
	4. Provide guidance for protection of confidential data and customer information;
	5. Provide guidance for proper records management (creation, storage, and disposition) on mobile devices;
	6. Be reviewed annually.
4. Agencies must provide training for employees explaining the agencies’ mobile device policies, including the following topics:
	1. Employee rights and responsibilities;
	2. Employees’ reasonable expectation of privacy for the types of devices used, as well as how to avoid disclosure of employee personal information;
	3. What constitutes a public record on a mobile device;
	4. Security measures the employee is expected to take to protect the mobile device and the public records stored there from theft, loss or unauthorized disclosure;
	5. Steps the employee must take upon request to make the device and its contents available for review, litigation, disclosure and records management, including:
		1. Unlocking the mobile device even if it is secured with a password or biometric identifier such as a fingerprint;
		2. Providing device to records management personnel for records inventory and assessment;
		3. Surrendering the device for a public records review;
		4. Surrendering the device during litigation;
		5. Returning a state-owned device when no longer needed;
		6. Returning the device when leaving employment with the agency.
	6. What kinds of mobile devices are appropriate for the employee’s job;
	7. Notifying the agency if a mobile device is lost, stolen, destroyed or compromised;
	8. Protecting client privacy and personal information in the course of public service.

Guidance: Using Mobile Devices

## Definitions

* Mobile Device: Any device capable of text, voice, email, instant messaging (“IM”), photo messaging or other types of data communication.
* Communication: Data including, but not limited to, text, IM, email; voice records and other records.
* Mobile Device Management (MDM): software that allows agency support staff to manage a “sandbox” or container on a mobile device where state data and applications can be added, deleted, or monitored.
* Enterprise Mobility Management (EMM): software that allows agency support staff to not only manage a container on the mobile device, but also control the flow of information between the mobile device and agency computing resources such as collaboration software, cloud storage, shared applications.

## What to Tell Employees

* State-Owned Devices
	+ Location Information: An employee shall have an expectation of privacy in personal physical location information generated by a state-issued device, unless such information is required for work purposes by the agency.
* Personal Devices
	+ An employee shall have an expectation of privacy in personal communications, but not work-related communications.
	+ If you create a message, document or image on your personal device about your work, it is most likely a public record.
	+ In the event a public records request asserts that a public record has been created on an employee’s personal device, the employee should expect to:
		- Surrender the device to the state/agency for a period of time;
		- Allow inspection of the device for the purpose of identifying and retrieving the public record pursuant to the request;
		- Make an affidavit certifying that he or she will identify all public records present on the personal device. Such records shall be subject to review or audit in the event of a litigation hold or public records request

## Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) Tools

* Agencies may require an MDM or EMM solution to fit their business needs;
* No specific MDM or EMM solution is mandated by OCIO;
* Personal devices with MDM or EMM installed on them are still personal devices and should be treated accordingly;
* Installing an MDM or EMM tool on a personal device does not relieve the employee of his or her obligations to preserve and produce records created or stored on the device.

Security Reminders

* Refer to OCIO [Policy 141.10](http://ocio.wa.gov/policy/securing-information-technology-assets-standards) (“Securing Information Technology Assets” http://ocio.wa.gov/policy/securing-information-technology-assets-standards) to answer questions about required security standards, including:
	+ Categories of data (public/sensitive/confidential/special handling);
	+ Security Design Review of agency applications; and
	+ Security training.
* Agencies must approve and document the use of category 3 data or above on mobile devices. This data must be encrypted.
* Mobile device functionality must not be modified to circumvent safety measures. The use of devices that are jailbroken, “rooted,” or have been subjected to any other method of altering or disabling built-in protections is not permitted.
* Pass codes used to secure mobile devices must:
	+ Be a minimum of six alpha numeric characters.
	+ Contain at least three unique character classes. Pass codes consisting of 11111a, aaaaa4, are not acceptable.
	+ Not contain more than a three consecutive character run. Pass codes consisting of 12345a, abcde1 are not acceptable.
	+ Render the device unusable after 10 failed login attempts.

Ethics Rules Apply

* State law (RCW [42.52](http://apps.leg.wa.gov/Rcw/default.aspx?cite=42.52)) and policies in most state agencies prohibit the use of public resources for private purposes; mobile devices are no exception. Using a state-issued mobile device for personal purposes (beyond “de minimis” use) is unethical in most circumstances.
* Employees should consult their agency ethics officer to make sure they understand what is allowed in specific situations.
* The Executive Ethics Board publishes advisory opinions on the use of state resources; [several opinions](http://ethics.wa.gov/search/google/cell%20phones) deal specifically with cell phones. For more information, see <http://ethics.wa.gov>.

## Training is Available

* The Office of Privacy and Data Protection offers training on protecting and preserving privacy in public service. <https://privacy.wa.gov>
* Mandatory security training reviewed by the Office of Cyber Security is available online or in person through the state’s [Learning Management System](https://gm1.geolearning.com/geonext/wasdop/dynamicopensite.geo?id=A/K6JkMT2OTaH/pKyR7t0Ru/U%2bH9rm6IrGdcdahcPZg%3d&nav=DOP_OS_Main) and the training office at the Department of Enterprise Services (<http://des.wa.gov/services/training-and-development>).