Policy & Standard Background

Name: Mobile Device Usage

New, Update or Sunset Review? Update

What is the business case for the policy/standard?

OCIO Policy 191 "Cellular Devices" was adopted in 2012, in response to specific concerns about the cost and flexibility of cellular phone service plans. Changes in public records law and the wireless service marketplace make the intent and language of the policy less relevant as a guide for agencies and policy makers. The security, privacy and records landscape pertaining to mobile devices requires a new approach and a new policy.

What are the key objectives of the policy/standard?

Establish a feasible risk, records and security floor for agencies to follow or build upon in managing mobile devices among staff.

Reduce the risk of improper records retention and disclosure for material created or stored on mobile devices.

Re-establish the primacy of the S.A.A.M. manual as the source of financial and reimbursement policies.

How does policy/standard promote or support alignment with strategies?

Recruit, Develop and Retain IT workforce – by allowing use of common, expected tools

Security and Privacy – reduce risks

What are the implementation considerations?

The proposed policy language will require more training for staff.
Each agency will be expected to study and adopt or enhance the OCIO policy to their own environment; this will take effort and thoughtful action.

Some provisions will be difficult to enforce on personal devices used for work.

Mobile Device Management solutions will be required; this will involve cost for agencies.

Agencies will have a year to come into compliance.

How will we know if the policy is successful?

Technology staff and records officers will have higher confidence in their ability to retrieve and produce data from mobile devices used for agency work.

Employees will experience less uncertainty about how to appropriately use mobile devices while preserving client and employee privacy.

More agencies will use MDM or EMM tools to manage data on mobile devices

CURRENT POLICY

PURPOSE

Ensure efficient assignment, use, and management of cell phones and related devices

POLICY STATEMENT

The state recognizes cellular devices, for certain 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.

The purpose of this policy is to help agencies:

- Ensure state-owned cellular devices and service plans are issued based on business needs;
- Ensure agencies and employees are aware of their responsibilities;
- Provide steps to improve state and agency cellular device management; Enable
- optimization strategies for devices and plans; and
- Establish policies to allow employees to use personal cellular devices.

1. Agencies Must Actively Manage State-Owned Cellular Devices
    - 1.1 Agencies must ensure assigned cellular devices and service plans are necessary for business needs, and continue to improve the purchasing, assignment, and monitoring of cellular devices and service plans.
    - 1.2 State provided cellular devices may be issued based on one or more of the following job requirements:
        - 1.2.1 Employee's job requires field work or travel where landline phones are inaccessible or inefficient;
        - 1.2.2 Employee's job requires immediate or on-call availability;
        - 1.2.3 Employee needs a cellular device for work-related safety, security, or other emergency reasons;
        - 1.2.4 Employee's job requires real-time communication, including email; or
        - 1.2.5 Other requirements as defined and documented by agency.
    - 1.3 The agency's authorizing staff and employee must complete Appendix A - Cellular Device Authorization and Agreement (or agency's equivalent) to document business need and policy acceptance.
    - 1.4 Agencies must work with the Department of Enterprise Services (DES) and cellular contractors, as necessary, to ensure state-issued devices are on the best plans for the lowest costs.
    - 1.5 Agencies must work with the Consolidated Technology Services (CTS) to ensure cellular devices such as smartphones, tablets, and data cards meet minimum requirements for compatibility and security.
2. Security, Privacy, and Records Management
    - 2.1 Employees must follow state security standards and are prohibited from storing or relaying confidential information by such means unless authorized by agency policy. Additionally, cellular device activity and transmissions may not always be secure.
    - 2.2 The state and agencies reserve the right to monitor the use of all state-owned cellular devices and services. Employees should not expect privacy in their use of state-owned equipment and services.
    - 2.3 All call records, documents and data, photos, etc. used to conduct state business via a personal device, and all contents of a state-owned device, are subject to records retention requirements and public disclosure. Any personal call records or other information may also be subject to review or audit in the event of a public disclosure request or litigation hold. Personal data (data on a personal device that does not constitute a public record) is not subject to public disclosure; however, all data on a state-owned device is deemed a public record (see section 4.1.3.)
    - 2.4 Agencies are responsible for managing and retaining public records related to cellular device usage in accordance with records retention schedules, including but not limited to billing and usage records.
    - 2.5 The cellular device must be wiped remotely when the device is lost or stolen, or when the maximum number of password attempts are made on the device, per the State IT Security Standards.
3. Agencies Must Optimize Devices and Plans

- **3.1 Agencies are required to optimize the use of state-owned devices and service plans. Optimization may include one or more of the following:**
  - **3.1.1 Combine service plan subscriptions, where possible, within agencies to streamline billing and**

management, and enable statewide optimization.

- 3.1.2 Ensure employees are using the most appropriate service plan. Monitor and analyze billing statements and usage reports regularly to identify potential savings and efficiencies.
- 3.1.3 Work with cellular contractors and agency employees to identify and deactivate or reassign unnecessary cell devices.
- 3.1.4 Use the lowest cost method for long distance calls and related telecommunications services.

4. Agencies May Authorize the Use of Personal Devices

- 4.1 Agencies may authorize employees to use their personal cellular devices to conduct state business when the following conditions are met:
  - 4.1.1 All employees who use a personal cellular device to access business documents and communications must comply with statewide and agency-specific security standards, records management and retention schedules, and all other applicable laws and standards.
  - 4.1.2 All call records, documents and data, photos, etc. used to conduct state business, and made via personally-owned devices, are subject to records retention requirements and public records disclosure.
  - 4.1.3 Personal call records and other information (e.g. personal data, photos, text messages, etc.) may be subject to review or audit in the event of a litigation hold or public disclosure request.
  - 4.1.4 The owner of a personal cellular device may be required to surrender the device, including all personal and business related information, if it is subject to a public records request or litigation hold.
  - 4.1.5 If the device is lost or stolen, or if a number of password attempts are made on the device, the cellular device will be subject to being wiped remotely (State Security IT Standards.)
  - 4.1.6 The agency's authorizing staff and employee must complete Appendix A - Cellular Device Authorization and Agreement (or agency's equivalent) to document business need and policy acceptance.

5. Agencies May Provide Stipends For Use of Personal Devices

- 5.1 An agency may authorize a monthly stipend for employees who use a personal cellular device in lieu of a state-issued device. Authorization is allowed only when an employee is required to use a cellular device for the conduct of state business based on job requirements (see section 1.2.)
  - 5.1.1 Monthly stipends are as follows:
    - Voice access $10 / month
    - Data access $30 / month
    - Voice and data access $40 / month
  - 5.1.2 The intent of stipends is to help minimize overall state cellular spend. The allowed stipend amounts were set by researching agency spending patterns, master contract prices, and market costs. The best attempt was made to calculate stipend amounts that do not exceed the actual cost to an employee for the service the state needs. Agencies may choose to reduce stipend amounts where appropriate.
  - 5.1.3 All stipends will be paid through a payroll transaction.
  - 5.1.4 Payroll taxes will be withheld if required by law. However, OCIO has determined that payroll taxes need not be withheld at this time on any stipend that complies with this policy.
- 5.2 An agency will not provide a stipend as a replacement for amounts previously treated as wages.
  - 5.2.1 An Authorization and Agreement terminates, and the agency will cease paying any stipend, when the first of the following events occurs:
    - Employee termination.
    - Agency ceases to have a business need for employee cellular access (see section 1.2.)
    - A decision to terminate the stipend for any other reason at the discretion of the agency or employee.
- 5.3 The employee is responsible to purchase the right device, service plan and coverage, to meet the agency's business needs (see sections 1.2 and 5.1.2.)
- 5.4 The agency is not responsible for the employee's cellular device or service plan.
- 5.5 The employee is responsible for costs and maintenance of the personal cellular device and service plan. The employee is also responsible for all contract fees such as activation and early termination, regardless of reason for Authorization and Agreement initiation or termination (see section 5.2.1.)
- 5.6 The employee receives and pays invoices directly for the cellular device and service plan.
- 5.7 An employee receiving a stipend must make their cell phone number available to agency employees and constituents for the purpose of contacting the employee during their regular working business hours, or no later than five business days after approval of the stipend or activation of the service plan, whichever comes first.
- 5.8 The agency's authorizing staff and employee must complete Appendix A - Cellular Device Authorization and Agreement (or agency's equivalent) to document business need, stipend amount, and policy acceptance.

RESPONSIBILITIES

Agency

- Agencies are responsible for ensuring the appropriate issuance and use of state-issued cellular devices and services, including employee eligibility, plan usage, and billing.
- Agencies may establish additional requirements for their employees that exceed these minimum policy requirements.
- When a cellular device is designated as shared, an individual within the work group must be assigned primary responsibility for the device.
- For state-owned devices, agencies must use the existing state contracts for state-owned cellular devices and services unless there are compelling business reasons to do otherwise (e.g. coverage, service or plan type, etc.)
- Agencies must designate who will review and approve requests for cell equipment and services consistent with these requirements.
- If the device is lost or stolen, or if a number of password attempts are made on the device, the cellular device (state issued or authorized personal cellular device) may be wiped remotely (State IT Security Standards.)
- Agencies are responsible for the review and approval of employee requests to use personal wireless devices as necessary to meet state business needs (see Appendix A.) At a minimum, agencies must establish procedures to monitor the on-going appropriateness of providing a stipend, and adherence to security requirements.

Employee

- Responsible for cellular device and proper use of the equipment in their possession as required by state and agency policies.
- Use the cellular device when it is the most cost effective and efficient communication method (e.g. versus desk phones, SCAN long distance, or state calling cards.)
- Review billing statements for accuracy as requested by their agency.
- Ensure records are retained in accordance with their agency's retention schedule.
- Employees in overtime eligible positions must document hours worked each day and each workweek. When an overtime eligible employee is issued a state cell phone or receives a cell phone stipend the supervisor and employee must ensure time spent on the phone for work purposes is included in the documented hours worked.
- Must notify their supervisor or appropriate management immediately in the event of damage, loss or theft of cellular devices. The employee must provide written notification within no less than three business days (see section 4.1.5.)
- While on state business, must comply with all laws applicable to use of hand held cellular devices (wireless communication devices) while operating a motor vehicle, including RCW 46.61.667 (no handheld devices) and RCW 46.61.668 (no texting.)
- Must return state-owned cellular devices to their supervisor immediately when the employee leaves position or is no longer an authorized to use a cellular device.
- Any employee using a state-owned device or their personal cellular device to conduct state business, whether the employee receives a stipend or not, must sign the authorization agreement or is in violation of this policy.

Department of Enterprise Services

- Provide master contracts offering the best options for cellular devices and service plans, for the lowest possible costs.
- Assist agencies in determining which plan may best fit their needs.
- Evaluate the plans offered under the Western State Contracting Alliance (WSCA) and determine if additional plans are needed. Procure additional plans as required.
- Provide ongoing, detailed state and agency billing and usage reports from each service provider to enable statewide cell phone optimization and cost transparency.

DEFINITIONS

Cellular device: A portable device with cellular communications capability and cellular service plan, such as a cell phone, smartphone, data card, cellular enabled tablet, netbook, or any other type of cellular device.

RELATED LAWS AND OTHER RESOURCES

Cell Phones and Service Plans - Department of Enterprise Services
http://des.wa.gov/services/cell-phones-and-service-plans [1]

Communications and SCAN Long Distance Services – Consolidated Technology Services
http://cts.wa.gov/products/Communications/SCANLongDistance.aspx [2]

Internal Revenue Service – Notice 2011-72 Tax Treatment of Employer-Provided Cell Phones
http://www.irs.gov/irb/2011-38_IRB/ar07.html [3]

Internal Revenue Service – Memo for Field Examination Operations #SBSE-04-0911-083
http://www.irs.gov/pub/foia/ig/sbse/sbse-04-0911-083.pdf

RCW 46.61.667 - Using a wireless communications device while driving
http://apps.leg.wa.gov/rcw/default.aspx?cite=46.61.667 [4]

RCW 46.61.668 - Sending, reading, or writing a text message while driving.
http://apps.leg.wa.gov/rcw/default.aspx?cite=46.61.668 [5]

State Administrative & Accounting Manual (SAAM) Chapter 75 – Uniform Chart of Accounts
http://www.ofm.wa.gov/policy/75.htm [6]

State Security Standards - Securing Information Technology Assets
http://ofm.wa.gov/ocio/policies/documents/141.10.pdf [7]

Records Management and Retention Schedules
http://www.sos.wa.gov/archives/RecordsManagement/records_state.aspx [8]

REVISION HISTORY

Date	Action taken
February to March 2012	Policy drafted.
April to May 2012	Policy endorsed.
June 26, 2012	Policy adopted.

CONTACT INFORMATION

For questions about this policy, please contact your OCIO Information Technology Consultant.

APPROVING AUTHORITY

/s/ Bharat Shyam **June 26, 2012**

Chief Information Officer **Date**
Chair, Technology Services Board

Source URL: https://ocio.wa.gov/policies/191-cellular-device-policy

Links:
[1] http://des.wa.gov/services/cell-phones-and-service-plans
[2] http://cts.wa.gov/products/Communications/SCANLongDistance.aspx
[3] http://www.irs.gov/irb/2011-38_IRB/ar07.html
[4] http://apps.leg.wa.gov/rcw/default.aspx?cite=46.61.667
[5] http://apps.leg.wa.gov/rcw/default.aspx?cite=46.61.668

[6] http://www.ofm.wa.gov/policy/75.htm
[7] http://ofm.wa.gov/ocio/policies/documents/141.10.pdf
[8] http://www.sos.wa.gov/archives/RecordsManagement/records_state.aspx
[9] http://www.governor.wa.gov/directives/dir_11-18.pdf
[10] http://Cell Phones and Service Plans - Department of Enterprise Services
[11] http://www.irs.gov/pub/foia/ig/sbse/sbse-04-0911-083.pdf

PROPOSED UPDATES TO POLICY

Policy No. 191- Mobile Device Usage

PURPOSE

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, records retention, the stewardship of confidential state information and related issues raised by mobile device usage.

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 state public records, 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.

POLICY STATEMENTS

1. State agencies have an affirmative duty under state law to retain, preserve exempt and non-exempt public records, and produce non-exempt public records in response to a request, including those created, accessed, used or stored on mobile devices. Agencies also have a duty to preserve and produce records for litigation purposes. Public records, both exempt and non-exempt, include those records – including, but not limited to, texts, voice mail, email, instant messaging, calendars, photos, and video – an employee prepares, owns, uses, receives or retains within the scope of employment. Agency mobile device usage policies must address and conform to these requirements.
2. An agency may approve expanded requirements beyond those identified herein to manage its mobile device program.
3. Agencies must determine which of the following mobile solutions their employees may use for agency business:
    - 3.1. State-owned and State-controlled Devices;
    - 3.2. Personal Devices
4. All mobile solutions used for state business must be equipped with up-to-date, currently-patched Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software;
5. Agencies must adopt a Mobile Device Policy and directly communicate that policy to each of their employees when revised
6. Agency Mobile Device Policies must:
    - 6.1. Govern employee use of mobile devices for agency business;
    - 6.2. Articulate employees' basic rights and responsibilities concerning mobile device usage;

6.3. Outline the process by which the agency receives access to public records prepared, owned, used or retained on mobile devices, including encrypted communications;
6.4. Provide guidance for protection of confidential data, records, and customer information;
6.5. Provide guidance for proper records management (creation, storage, and disposition) on mobile devices;
6.6. Undergo annual agency review for possible update.

7. Agencies must provide training for employees explaining the agencies' mobile device policies, including but not limited to the following topics:
   7.1. Employee rights and responsibilities;
   7.2. Privacy concerns for the types of devices used, as well as how to avoid disclosure of employee personal information;
   7.3. What constitutes a public record on a mobile device;
   7.4. 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;
   7.5. Steps the employee must take upon request to make public records on the device and its contents available to the agency for review, litigation, disclosure and records management;
   7.6. What kinds of mobile devices or solutions (if any) are prohibited under agency policy;
   7.7. How to notify the agency if a mobile device is lost, stolen, destroyed or compromised;
   7.8. Protecting client privacy and personal information in the course of public service.
8. Agencies must comply with this policy by June 30, 2019.

Definitions

- Mobile Device: Any hand-portable device capable of text, voice, email, instant messaging ("IM"), photo messaging or other types of data communication. This policy is not meant to apply to: cars, boats, airplanes, laptop computers, desktop computers, unpiloted aerial vehicles (drones), gps receivers, radios.
- Communication: The exchange or sharing of 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. Additional functions may include: issuance, inventory tracking, policy enforcement on the device.
- 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. Additional

functions may include: issuance, inventory tracking, policy enforcement on the device.

CONTACT INFORMATION:

Contact the OCIO Policy & Waiver Mailbox if you have questions about this policy.

SUNSET REVIEW DATE: **May 11, 2021**

ADOPTION DATE: **May 11, 2018**

APPROVAL DATE: **Targeted Date is June 12, 2018**

APPROVING AUTHORITY: Rob St. John, Acting State CIO & Chair of TSB

Name	Org	Regarding	Comment	Received	Via	Disposition
Baird Miller	ECY	General	My first reaction is that the scope is good, but it is very prescriptive… statewide policies tend not to be so prescriptive because it actually adds risk if we don't follow it to the details provided….	9/11/17	email	
Harold Goldes	DES	Records	Guidance: I suggest we assume that it <u>is</u> a public record. Whether it will be disclosed depends on the specific public records request. Guidance: I suggest the three use cases are: 1. State Owned Device 2. Personal Device for which employee receives a "stipend" in consideration for which the employee agrees (i) to allocate some portion of the device resources (e.g., bandwidth, storage) to agency use (ii) permit agency to search allocated resources for records responsive to a PRR 3. Personal device: (see below)	9/11/17	email	Retain current language on use case 2 – the team and commenters prefer MDM as a technology <u>requirement</u> on all personal devices, regardless of stipend
Harold Goldes	DES	Records	Guidance: i'm not sure the burden is on the PRR to identify the record's location; a diligent thorough search would be reasonably calculated to locate responsive records and as such examine all locations where such records reside. Otherwise a mobile device search could depend on the requestor knowing of the existence/ use of such a device Guidance: Surrender the device to the state/agency for a period of time; Not necessarily: The guidance here is that "an employee's good-	9/11/17	email	Clarify the Guidance language to indicate that it is the <u>search</u> for records that reveals records on a device, not the request itself.

			faith search for public records on his or her personal device can satisfy an agency's obligations under the PRA. The agency bears the burden acting thorough its employees—to perform "an adequate search" for the records requested. (see Neigh. All., 172 Wash.2d at 720–21, 261 P.3d 119) The agency's burden is to show that the agency conducted an adequate search for records. That burden may be satisfied if the employee submits, in good faith "reasonably detailed, nonconclusory affidavits" attesting to the nature and extent of their search. Id. at 721, 261 P.3d 119.			
Harold Goldes	DES	Affidavits	A court may resolve disputes about the nature of a record "based solely on affidavits," RCW 42.56.550(3), i.e. without an in camera review, without searching for records itself, and without infringing on an individual's constitutional privacy interest in private information he or she keeps at work. Note on requirements of any affidavits: the affidavit must give the requester and court a sufficient factual basis to determine that withheld material is indeed nonresponsive, the agency has performed an adequate search under the PRA. (it's kind of analogous to an exemption log which must give the requestor a clear map of what is omitted and why)			Retain present language in Guidance – affidavits are not dispositive in all cases
Alyson Brooks	DAHP	Records	Harold - I think there is a difference between what the courts have decided and the right of the state to determine its own	9/11/17	email	Retain present language

			policy of when allowing an employee to use their own phone. Seems to me if we are going to allow an employee to use their private phone for government business..then the state should reserve the right to have it inspected by a public records officer if necessary. The use of one's own phone is optional, not required. The state really needs to protect itself under the PRA from large fines due to someone not sharing a record.			
Harold Goldes	DES	Records	Good point. Technology develops way faster than case law. My limited experience is that employees will use personal mobile devices, rarely out of devious motives or to evade public disclosure law. In such cases what are an agency's options? In late 2017, affidavits documenting an employee "self search" of a personal device seem like a collision avoiding balance between an employee's real or perceived right to privacy in their own property and an agency's need to conduct a thorough search to avoid fines and fees. H	9/11/17	email	Retain present language
Belinda Girard	DOL	Access to device	not clear on this statement: Ensure that the agency receives access to public records produced or stored on mobile devices, including encrypted communications	10/23	Doc	Retain present language
Gary Nicholas	DOL	Personal device	How do we enforce this control? (An employee shall have an expectation of privacy in personal communications, but not work-related communications.) I would be highly concerned about my personal device privacy.	10/23	Doc	Retain present language – team and most commenters concluded that employee

						privacy does not extend to work records on personal device
Gary Nicholas	DOL	Personal device	This (surrendering device to records officer) has to be clearly defined if someone's personal device is to be withheld. The impact on an individual's personal life can be significant (family emergency, etc.). My concern – this can backfire in a safety situation.	10/23	Doc	Retain language in Guidance
Vel Rajagopal	DOL	Personal Device	Should we now draft an affidavit and have everyone in DOL who is subsidized, sign it?	10/23	Doc	Retain present language – this is agency discretion, to be implemented in agency policy as directed by agency Public Records Officer
Ron Anderson	DOL	Device agreement	All staff who request a state-owned device or use their personal device are currently required to fill out and sign a "Wireless Cellular Device Agreement". Part of that agreement states that they have read the agency "Wireless Cellular Device for Agency Business Policy" (IT Policy 5.1.1) The policy states that employees who use a personal WCD for DOL business will comply with the employee requirements of OCIO policy 191(4).	10/23	Doc	Noted – no action required
Vel Rajagopal	DOL	MDM	No specific MDM is mandated -- This is great. We do not have to work with WaTech's AirWatch offering. There are much better offerings such as MaaS360.	10/23	Doc	Noted -- No action required
Vel Rajagopal	DOL	MDM	Could DOL enforce using a messaging tool that will record messages and store them, if	10/23	Doc	Yes – that is an option

			employees use them for state business use? Eg. Tiger text			
Vel Rajagopal	DOL	Encryption	For DOL's purposes, we should just not allow any data other than Cat 1 or 2. Is there any nuance in just prohibiting Cat 3 or 4 transmission on mobile devices?	10/23	Doc	Noted -- No action required
Gary Nicholas	DOL	Encryption	This can be challenging. Data is usually co-mingled with several categories. We can prohibit the use of cat 3/4 but would need an enforcement mechanism.	10/23	Doc	Noted -- No action required
Gary Nicholas	DOL	Pass codes	Do we have the capabilities to enforce these controls today? If not, we should gather these as requirements for an MDM solution.	10/23	Doc	Guidance; no action required
Chris Foster	LNI	Communicate to employees	Need to clarify if this is all staff or only staff with mobile devices. What does "Ongoing basis" mean? Yearly, as changes are made?	10/27		Delete phrase
Chris Foster	LNI	Training	How frequently must training be done? Again, all employees or just mobile device users?	10/27		Retain; yes the policy requires training for employees who do not use state cellphones
Chris Foster	LNI	Training	This should be covered employee responsibility. The below steps are too granular for a state level policy. Agencies should create their own policies to cover this. Additionally, agencies should train to the policy. There should not be a separate section saying what to put in the training.	10/27		Retain
Chris Foster	LNI	Location	Is it their physical location or their residential location that is protected?	10/27		Clarify – add "residential"
Chris Foster	LNI	Records Guidance	If you create a message, document or image on your personal device about your work, it is most likely a public record -- It is a public record at that point	10/27		Clarify – remove "most likely"

Chris Foster	LNI	Security guidance	"Agencies must approve and document the use of category 3 data or above on mobile devices. This data must be encrypted." This should be reflected in the above policy	10/27		Decline: need to avoid overlap with 141.10
Chris Foster	LNI	Passcodes guidance	minimum of six alpha numeric characters. How would this be enforces on a personal device?	10/27		Remove guidance
Rick Griffiths	ATG	Basic rights	4.1. Employee rights and responsibilities; Was there an intended difference between basic rights and rights?	9/12		Harmonize language in 4.1
Mike Callahan	WaTech	Expectation of privacy guidance	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. – Not sure about case law on this	9/30		
Mike Callahan	WaTech	Records guidance	If it's about work, it is a public record – i.e. if it's a record prepared, owned, used, or retained by an agency relating to the conduct of government.	9/30		
Marie Finn	DSHS	MDM	Is it assumed state-owned devices will have management software? This leaves it open to interpretation.	11/1	Doc	Clarify: MDM is agency's option but recommended by OCIO
Marie Finn	DSHS	Communicate to employees	What is the expectation of privacy? That an agency is not collecting this information or that the agency is collecting this information but will not disclose it to a 3rd party?	11/1	Doc	Remove guidance
Marie Finn	DSHS	MDM	Any mobile device that is used in any capacity for the State should have either MDM or EMM. Leaving which is used to the agencies is fine, but it appears that it's optional.	11/1	Doc	
Marie Finn	DSHS	Encryption	Does this mean that data must be encrypted on the device, but in transit to the device it is not required to be encrypted. For	11/1	Doc	

Commented [CM(1]: I'm not sure about this. DES had a recent issue with telematics vis-à-vis public records. I don't know if there's any case law about this.

			example, DSHS clients may text to state employee devices.			
Marie Finn	DSHS	Security	Mobile device functionality must not be modified to circumvent safety measures -- Don't see a similar statement in OCIO Policy 141 or 141.10 about not modifying or altering, but recommend something is added to them rather than just in the "guidance" section of this policy.	11/1	Doc	Recommend new language for 141.10
Carrie Basas	OEO	Encryption	Anonymous 2mo The policy draft says that cat3 must be encrypted. Is that only true/available with MDM? Our staff only uses state-issued mobile devices. Carrie Basas, OEO Director	9/2	Web	Clarify: encryption in OS is ok
John Specht	HCA	Training	*HCA has concern about the requirement that agencies must provide training on mobile devices. We touch on related concepts in privacy and security trainings already. And soon, we will also touch on related concepts in telework, records retention, and public records trainings. A mobile device-specific training seems like overkill and we'd prefer an enhanced user agreement that conveys the same points.* John Specht - HCA	9/2	Web	Clarify: covering these topics in standard training is sufficient
Anon	NA	Location	Since the location of state employees homes are not subject to disclosure, are any additional considerations needed to account for that?	9/18	Web	

Anon	NA	Definition of Device	*The current definition of mobile would include every type of computer, including the towers and desktop models. The mainframe communicates data, and can store, receive and send multimedia (audio, photo, video, email, etc.). A better definition may be helpful.. current definition is: • Mobile Device: Any device capable of text, voice, email, instant messaging ("IM"), photo messaging or other types of data communication.*	10/20	Web	Confirm expanded definition
Brian Cochran	SCC	Agency Policy	1) Rather than having each agency develop their own policy, we'd prefer if OCIO put out a policy in a form that we, the smaller agency, could point to. We're a whole 21 folks strong, without a dedicated CIO or IT staff. We've noticed an uptick in the number of policies we must develop to comply with OCIO directives (the latest being accessibility). While we understand the need for the policies, it takes our non-IT trained staff considerable time and valuable skills away from our agency mission-related work.	10/31	email	OCIO will add a model small-agency policy to guidance
Brian Cochran	SCC	OCIO authority	Rather than a series of isolated policies from different silos of OCIO, we'd like to see one covering everything, rather than a new policy requirement when each OCIO shop develops their own requirement.			Referring this suggestion to the CIO and TSB
Brian Cochran	SCC	OCIO authority	It appears that several policy requirements related to mobile devices may overlap with other policies that we're required to have. We'd prefer to modify an existing policy rather than have a bunch of overlapping policies.			Retain: we think the seeming overlap areas are in Guidance, not policy.
Mark Lyon	ATG	Purpose	The scope of employee privacy in this context is very broad, not	11/6/2017	Markup	Removed purpose

			well defined and variable depending upon the facts. It is not reasonable for the OCIO or Agencies to articulate the scope of this privacy, which is ultimately the work of courts.			statement element
Mark Lyon	ATG	New section	State agencies have an affirmative duty under state law to retain, preserve and produce non-exempt public records, including those created, accessed, used or stored on mobile devices. Public records include those records – including texts, voice mail, email, instant messaging, calendars, photos, and video – an employee prepares, owns, uses, or retains within the scope of employment. Agency mobile device usage policies must address and conform to these requirements.	11/6/2017	Markup	Added to policy section
Mark Lyon	ATG	New section	Agencies should manage mobile device usage in a secure manner consistent with the requirements of OCIO Policy No. 141 - Securing Information Technology Assets and OCIO Standard No. 141.10 - Securing Information Technology Assets Standards. Mobile Device use, including the use of personal devices, where authorized, should be included in the agency risk assessment of Information Technology Assets.	11/6/2017	Markup	Add to guidance. The policy statement is generally a "must", whereas this item is explicitly a "should"
Mark Lyon	ATG	Agency policy	Agency Policy must address at least the following three use scenarios for devices their employees may use on the job: … In fact, there can be multiple use scenarios for mobile devices, and they can be mixed and matched. …"category" may be too ridged a work here, since there are many possible use scenarios (some of which would not be prudent to adopt).	11/6/2017	Markup	Revised policy, substituting "Solutions" for "types of devices"

Mark Lyon	ATG	Agency policy	"Provide guidance for protection of employee privacy,"	11/6/2017	Markup	Retain. "Guidance" is implied in "Articulate employees' basic rights,"
Mark Lyon	ATG	Training	These listed items are theoretically possible but are unlikely when dealing with a personal device. *Nissen v. Pierce County*, 183 Wn.2d 863,878-879, 886-887 (2015); West v. Vermillion, 196 Wn.App. 627, 635-636 (2016). In Nissen, the court held that where a public agency received a Public Records Act request for an employee's text messages on work-related matters sent and receive from a private cell phone ("public records") the agency should proceed as follows: "Therefore, we hold agency employees are responsible for searching their files, devices, and accounts for records responsive to a relevant PRA request. Employees must produce any public records (e-mails, text messages, and any other type of data) to the employer agency. . . . Where an employee withholds personal records from the employer, he or she must submit an affidavit with facts sufficient to show the information is not a "public record" under the PRA. So long as the affidavits give the requester and the trial court a sufficient factual basis to determine that withheld material is indeed nonresponsive, the agency has performed an adequate search under the PRA. When done in good faith, this procedure allows an *887 agency to fulfill its responsibility to search for and disclose public records without unnecessarily treading on the constitutional rights of its employees." 183 Wn.2d, 886-887	11/6/2017	Markup	Removed specific training elements. Case law makes OCIO policy specifics inappropriate.

Mark Lyon	ATG	Guidance / Definitions	What about GPS on State Vehicles? Internet of Things (IOT) with GPS or other data connectivity?	11/6/2017	Markup	Added clarifying language to definition of "Mobile Device" excluding vehicles, laptops, gps, etc.
Mark Lyon	ATG	Guidance / What to Tell Employees	This seems too narrow for a complicated subject addressed in this Guidance. In addition, "what to tell employees" will depend upon the scenario and the device. There will not be a one size fits all. Perhaps focus should be on what kinds of considerations should go into an agency policy? Use of "personal devices" at work is frequently referred to as a "Bring Your Own Device" or BYOD policy. Do we want to reference this to make clear what we are talking about? See previous comment about agency ability to grant an "expectation of Privacy" contrary to the PRA or other requirements. Otherwise the statement is basically true, especially in the context of personal devices. As noted in *Nissen*, "an individual has no constitutional privacy interest in a public record" – a record prepared, owned, used, or retained by an agency employee acting within the scope of employment. But "records an employee maintains in a personal capacity will not qualify as public records, even if the refer to, comment on, or mention the employee's public duties." 183 Wn.2d, at 881 n.8, 883. Note however that the question about whether a record is "personal" (i.e., not a public record) and whether the employee has a privacy interest in that record are two different issues. Other factors will determine whether the employee has a reasonable	11/6/2017	Markup	Deleted section "What to tell employees"

			expectation of privacy in "personal" records (e.g. personal emails on a state-owned device) that the individual can enforce against his employer or third parties. *See Nissin*. This statement is a gross over-simplication of complicated legal principles. For example, an employee may need to disclose deeply personal information in leave records, etc. and would not be able to assert a "right to privacy" against the employer. However, the same employee might be in a position to assert a right to privacy against a third party.			
Agnes Kirk	OCS	MDM	Personal devices without basic MDM capabilities are no longer an acceptable cyber risk; the policy should establish a stronger baseline expectation of agency actions.	1/4/2018	Meeting	Revised policy and guidance to require MDM or its functional equivalent.
Anita Wieland	OFM	Purpose	Consider including language similar to: An agency may approve expanded requirements beyond those identified herein to manage its mobile device program.	3/23/18	Document edits	
Nathan Sherrard	OFM	Training	need to be cautious with these kinds of statements (about employees' privacy expecatations or lack thereof). A court could order an employee to surrender a personal device, but an agency, I doubt it.	3/23/18	Document comment	
			I am extremely doubtful that an agency can require an employee to unlock and turn over a personal device for unfettered "records inventory and assessment."	3/23/18	Document comment	
Tracy Guerin	TSB	Schedule	Agencies should have time (about a year) to come into compliance.	5/10/2018	Subcommittee meeting	Added to policy.