OREGON YOUTH AUTHORITY
Policy Statement
Part I – Administrative Services

Subject:

Mobile Communication Devices (Cell Phones) and Other Mobile Data Storage Devices

Section – Policy Number:	*Supersedes:*	*Effective Date:*	*Date of Last Revision/Review:*
C: Property Management – 9.0	**I-C-9.0 (06/13)** **I-C-9.0 (06/10)** **I-C-9.0 (09/08)** **I-C-9.0 (06/03)** **I-C-9.0 (02/99)**	**12/21/2018**	**None**

Related Standards and References:

- DAS 107-001-0015 (Internal Controls for the Management of Mobile Communication Devices)
- Department of Administrative Services, Information Resources Management Division (DAS-IRMD), Oregon Statewide IT Policies
- Department of Administrative Services, Enterprise Information Strategy and Policy: 107-004-051 (Controlling Portable and Removable Storage Devices)
  107-009-0050 (Sustainable Acquisition and Disposal of Electronic Equipment)
  107-001-015 Internal Controls for the Management of Mobile Communication Devices
- OYA policy: 0-7.0 (Use of Electronic Assets and Systems)
  I-C-2.0 (Use of State-owned Vehicles)
  I-C-1.0 (Property Control Systems)
  I-E-1.4 (Public Records Management)
  I-E-2.0 (Records Retention, Destruction and Archiving)
  I-E-2.3 (Requests for Youth Information and Records)
  I-E-3.2 (Information Asset Classification and Protection)
  I-E-3.3 (Information Security Incident Response)
  II-A-1.0 (Facility Access)
  II-A-3.1 (Youth Transports)
- OYA forms: YA 8023 (State Mobile Device Acquisition - User Agreement)
  YA 8026 (Authorized Personal Mobile Device User Agreement)
  YA 8021 (Employee Agreement on Electronic Communication and Information Assets)
  YA 8110 (Employee-assigned Property)

Related Procedures:

- None

Policy Owner:

Chief Information Officer

Approved:

Joseph O'Leary, Director

I. PURPOSE:

This policy provides standards for OYA staff in protecting OYA information stored on mobile data storage devices. The policy also delineates how OYA manages state-owned mobile communications devices.

II. POLICY DEFINITIONS:

Authorized Mobile Data Storage Device: A state-owned or personal mobile data storage device approved for state business use.

Critical Information: Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

Limited information: Sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, partners. OYA must follow its disclosure policies before providing this information to external parties.

Mobile Communication Device (MCD): A text messaging device or wireless, two-way communication device (cell phone) designed to receive and transmit voice or text communication, including mobile Global Positioning Systems (GPS) and smart phones.

Mobile data storage device: An electronic device that stores data and is designed for portability (e.g., mobile communication device, laptop, USB flash drive, CD, DVD, tablet, gaming device, MCD).

Restricted Information: Restricted information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency prior to receiving it.

III. POLICY:

OYA physically controls and protects mobile data storage devices, and protects and manages any information stored on them. The controls protect against theft of state-owned equipment, unauthorized disclosure of information, misuse of equipment or unauthorized access to information and devices.

Generally, OYA information will be stored on the OYA network. Staff may load OYA information onto OYA-authorized mobile data storage devices as needed to do their immediate work. Staff may only take the amount of OYA information off site needed to perform their duties.

See OYA policy I-E-3.2 (Information Asset Classification and Protection) regarding how different sensitivity levels of information must be protected.

State-owned or approved personal Mobile Communications Devices (MCD) may be used for state business when the use supports OYA business interests and is economically justified. Only those whose job functions require use of an MCD may be issued state-owned MCDs and are authorized users for plan charges. OYA will only pay MCD plan charges for authorized users.

Failure to comply with any provision of this policy or standards contained within may result in disciplinary action, up to and including dismissal from state service.

IV. GENERAL STANDARDS:

A. Staff must connect to the secure OYA wireless access point when using an authorized mobile data storage device whenever an OYA wireless access point is available.

B. Conversations and text messages via authorized mobile data storage devices must be limited to non-restricted and non-critical information when possible. If restricted or critical information is discussed or written, staff must attempt to do so out of sight or hearing range of others.

C. Staff must ensure the authorized mobile data storage device is password protected at sign-on.

D. Staff must ensure the authorized mobile data storage device is locked in a drawer, cabinet, or room when not in use.

E. Staff must ensure the authorized mobile data storage device is encrypted, if capable.

F. Staff must ensure youth do not use or access staff MCDs or mobile data storage devices.

G. OYA reserves the right to delete **all** information from an authorized mobile data storage device if a staff member's employment with OYA ends, or the staff member's authorized mobile data storage device is lost, stolen, or replaced.

1. Staff must immediately notify a supervisor (or officer-of-the-day) and call the Information Services Service Desk, (503) 378-4333 (option 2), if the device is lost, stolen, replaced, or no longer needed for OYA business.

   Refer to OYA policy I-E-3.3 Information Security Incident Response for additional instructions if the lost or stolen device contains restricted or critical information.

2. Human Resources must immediately notify the Information Services Service Desk of a staff member's separation from OYA on or before the staff member's separation date.

H. Information stored on authorized mobile data storage devices is subject to public records laws.

OYA may need access to an authorized mobile data storage device to obtain data or information in the event of a personnel or criminal investigation concerning an OYA matter.

I. Authorized MCDs

1. Staff must carry an authorized MCD when transporting youth, and when conducting youth home visits.

2. Staff must use a hands-free accessory when driving a vehicle while using an authorized MCD.

a) Staff are advised to use extreme caution when using an MCD while driving a vehicle due to an increased potential for vehicle accidents while driving and using an MCD.

The preferred method to use an MCD while operating a vehicle is to park the vehicle in a safe place prior to using the MCD.

b) Any traffic violations or payment of fines imposed for violation of any applicable laws including those on MCD use is the staff member's personal responsibility.

J. Staff must not store OYA information on unauthorized personal mobile data storage devices.

V. PURCHASING AND CONTROLLING STATE-OWNED MCDs

A. An Information Services staff member is designated as the OYA's mobile communication plan coordinator.

1. The mobile communication plan coordinator -

a) Is authorized to open, manage, and cancel authorized MCD accounts;

b) Is authorized to purchase all MCDs for OYA;

c) Serves as the contact and liaison with Department of Administrative Services (DAS) and the vendor;

d) Ensures that access services for lost or stolen MCDs are disconnected; and

e) Maintains a list of all MCD access accounts and corresponding authorized users (staff names) and any special purpose accounts.

2. Supervisors must request MCDs and services through the mobile communication plan coordinator by creating an IS work order.

B. Supervisors will determine if a staff member needs to use a state MCD to perform job duties.

1. Valid reasons to need a state MCD include –

a) Official duties require the staff be “on-call” away from workstations;

b) Official duties require extensive travel during the staff’s normal assigned work time;

c) Official duties expose staff to off-worksite danger; or

d) Official duties require an emergency or time-critical response.

e) Cost of device is justified by the gain in operational efficiency.

2. Worksite MCDs may be distributed by the worksite supervisor when deemed appropriate by that supervisor.

C. Review of state-owned MCD billing

Accounting will audit monthly billings to identify potential inappropriate use of the MCD and any billing errors.

D. Appropriate use of state-owned MCDs

When staff are designated as authorized users of a state-owned MCD, such use is intended for state-related business. However, limited incidental personal use is allowed as long as there is no or insignificant cost to the state.

1. OYA has the sole discretion to determine if a staff’s use is personal or business.

2. Staff may be required to reimburse OYA for unauthorized personal use of an MCD.

E. Refer to OYA policy II-A-1.0 (Facility Access) for guidelines on carrying MCDs into OYA facilities.

F. Supervisors will ensure the staff they authorize to use state-owned MCDs understand acceptable use of the MCD, and the staff receive a copy of this policy prior to using state-owned MCDs.

1. Staff must document their acknowledgement and receipt of the policy on OYA form YA 8023 Mobile Communication Device Acquisition - User Agreement.

2. Supervisors must keep a current list of all assigned state-owned MCDs and the staff authorized to use such MCDs.

VI. CONTROLLING STATE-OWNED MOBILE DATA STORAGE DEVICES

A. Assigning state-owned mobile data storage devices (other than MCDs)

1. Assignment of state-owned mobile data storage devices must be documented on a YA 8110 (Employee-assigned Property) form.

2. The document must describe the device, who it is assigned to, the location of the worksite, the date assigned, and the supervisor responsible for the device.

3. The documentation must be kept current and retained for two years after the state-owned mobile data storage device is returned.

B. Transporting state-owned mobile data storage devices

1. Staff must have authorization to remove the storage device from the worksite. Authorization is contingent upon work assignment and local protocol.

2. Related protocols on logging removable storage devices must be followed (e.g., signing for a laptop).

3. Transporting in vehicles

a) Staff will maintain physical control of the mobile data storage device throughout the transport and ensure protection from view by unauthorized people.

b) If the mobile data storage device must be left unattended in a vehicle, the vehicle must be locked and the device must be out of plain sight (preferably in the vehicle's locked trunk).

C. Shipping state-owned mobile data storage devices

Mobile data storage devices containing critical or restricted information may be shipped when the following conditions are met:

1. Secure tape, sealant, or other tamper-evident material is used to identify a breach of the package; and

2. The people who have a need to know of the shipment are identified.

a) Pre-agreed receiving names are authorized for signature at the destination.

b) Post-alert confirmation of delivery to recipient is ensured upon delivery (e.g., recipient contacts the sender upon the package's arrival).

c) Passwords are identified in a separate communication. Staff may not identify the related password in the same communication that mentions the specific mobile data storage device.

D. Intergovernmental agreements on sharing restricted or critical information on mobile data storage devices must be followed.

E. Disposal of mobile data storage devices

1. Staff must deliver or mail OYA mobile data storage devices to the Information Services Service Desk for disposal.

2. Information Services must follow the statewide policy on Sustainable Acquisition and Disposal of Electronic Equipment (DAS policy 107-009-0050).

3. When mailed, staff will notify the Information Services Service Desk via e-mail of the number of devices and date shipped.

4. The Information Services Service Desk will confirm receipt and destruction of the devices.

VII. PERSONAL MOBILE DATA STORAGE DEVICES

If authorized, staff may use their personal mobile data storage devices for business purposes only if the use supports OYA business interests.

A. Staff are responsible for all costs incurred while using the device for business purposes.

B. Staff must read and sign OYA form YA 8026 (Authorized Personal Mobile Device User Agreement) prior to using a personal device for business purposes. The signed YA 8026 will document the staff's acknowledgement and receipt of this policy.

C Information Services will keep a list of all personal devices that are authorized to be used for business purposes.

D. Staff must comply with the general standards listed in part IV of this policy.

E. Business-related information stored on a personal mobile data storage device is subject to public records laws. See OYA policy

I-E-1.4 Public Records Management regarding text and e-mail record management.

VIII. LOCAL OPERATING PROTOCOL REQUIRED: NO