MOBILE DEVICE POLICY

Policy Number: TEC-103

Effective Date: Approved by the **Eastern Washington State Historical Society (EWSHS)** Board of Trustees on July 1, 2020.

Application: Applies to all employees of EWSHS (Eastern Washington State Historical Society)

History: This is a new Board Policy.

Article I
PURPOSE

1.1 This policy defines and establishes procedures to ensure the efficient assignment, proper use, and effective management of mobile devices (state issued or personally-owned) for the EWSHS.

Article II
POLICY APPLICATION

2.1 This policy applies to all EWSHS employees who have been authorized to use a state-owned or personally-owned mobile device to conduct state business for the EWSHS.

Article III
DEFINITIONS

3.1 **Container:** Mobile Application Containerization is the process of putting applications in containers with an operating environment all its own; company information is kept separate from personal information on phones and tablets and applications are isolated to prevent intruders, malware and other applications from compromising the network.

3.2 **De Minimus**: Lacking significance or importance, so minor as to merit disregard.

3.3 **Employee**: Permanent, temporary, or volunteer worker.

3.4 **Executive Director**: The director of the EWSHS functioning within the authority to set agency direction and implement internal policy.

3.5 **Mobile Device**: Mobile computing devices are modern-day handheld devices that have the hardware and software required to execute typical desktop and Web applications allowing data to be viewed, edited, transmitted, received or recorded while away from the office. Among common examples of mobile devices are cellular phones, tablets, cameras, GPC, mobile printers, and portable data storage devices such as removable hard drives.

There are two classifications of mobile devices:

a. Employee-Owned Device: Refers to mobile devices procured by the employee, with no connection or association with the EWSHS. Employee-owned devices do not have access to any state-owned computing resources, with the exception of EWSHS email via that appropriate containerized connection. Approved employees, as part of the approval process, and as permitted by the budget, may qualify to have the cost of their personal device ownership and usage partially offset by a monthly stipend. All other costs of the device ownership and usage are paid for by the employee. See BP#146 for further information.

b. Agency-Issued Device: A mobile device procured by the agency and issued to employees for the purposes of conducting company business with full access to privileged state-owned computing resources. All costs associated with the agency-issued device are paid for by the agency.

3.6 **Mobile Device Management:** Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) is a widely used term describing device management and other mobile management functions including operations, policy, security, configuration, application support (application performance, version control, distribution, etc.), mobile data management and some mobile network monitoring.

3.7 **Public Record:** Public record includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. A record may be a "public record" even if created or stored on an employee-owned device.

3.8 **State Government Network (SGN)**: SGN is the State of Washington's security boundary for its enterprise, managed internal network that is built around internet technologies, security, and standards (such as Office of the Chief Information Officer (OCIO) Policy 141.20) to enable participating agencies to share mission critical applications and data within the statewide private network.

3.9 **State-Owned Computing Resources**: Any computer hardware, software, data, or network resources that the EWSHS makes available to its employees.

a. Computer Hardware: Desktop and laptop computers, monitors, hand-held computing devices, smart phones, printers, plotters, servers, and other types of electronic devices which are capable of being connected to an EWSHS computer or network.
b. Computer Software: Operating system software; commercial, open source or public domain application software; and EWSHS developed application software.
c. Computer Data: Information stored electronically, whether routers, modems, network servers, network operating system software, email systems, data and phone lines, and connections to other computers and the internet.

3.10 **Transitory Records:** Temporary information (less than 180 days) that isn't required to retain in order to meet legal or fiscal obligations, or to initiate, sustain, evaluate or provide evidence of decision making to conduct business.

Article IV
STATE-OWNED MOBILE DEVICE REQUESTS/DECISIONS

4.1 The availability of state-owned mobile devices is dependent on the EWSHS budget and the discretion of the Executive Director.

4.2 If EWSHS employees believe they have a need for a state-owned mobile device, and the EWSHS budget allows for it, then they may make a request in writing to the Executive Director. The Executive Director will ensure that an appropriate business need is present prior to issuing a state-owned device to an employee.

4.3 Only state-owned mobile devices will have the authority to conduct EWSHS official business or to access EWSHS records via remote access, authorized by the Executive Director and set up by EWSHS IT employees.

4.4 State-provided mobile devices may be issued based on one or more of the following job requirements:

a. Employee's job requires field work or travel where landline phones are inaccessible or inefficient;
b. Employee's job requires immediate on on-call availability;
c. Employee needs a mobile device for work-related safety, security, or other emergency reasons;
d. Employee's job requires real-time communication, including email; or
e. Other requirements as defined and documented by the EWSHS.

4.5 Prior to being issued a state-owned mobile device to conduct agency business, the employee and Executive Director must complete a Mobile Device Authorization and Agreement form to document business need and policy acceptance. See Appendix A for the Mobile Device Authorization and Agreement.

Article V
EMPLOYEE USE OF AGENCY-ISSUED MOBILE DEVICES

5.1 The employee will be subject to the following:

a. All agency-issued mobile devices must be enrolled in the agency MDM or EMM system.
b. All records, including call records, videos, text messages, photos, and internet usage history on agency-issued devices are the property of the EWSHS and subject to records retention requirements, litigation holds and public records disclosure.
c. Agency-issued devices may be reviewed or audited in the event of an HR investigation, litigation hold, or public records request.
d. The Ethics in Public Service Act, chapter 42.52 RCW, prohibits the use of public resources for private purposes. Mobile devices are no exception. Using state-owned mobile devices for personal use, beyond "de minimus" use, is unethical in most circumstances. An employee may make occasional, but limited, personal use of state-owned mobile devices under the following conditions:

I. There is little or no cost to the State.
II. Any use is brief.
III. Any use occurs infrequently.
IV. The use does not interfere with the performance of an employee's official duties.
V. The use does not compromise the security or integrity of state-owned computing resources.

e. Agency-issued devices will be returned to the agency when the employee is separated, when the device is no longer needed, or when it has reached end-of-life.
f. Employees may not install unapproved mobile applications on agency-issued devices.
g. Tampering with the agency-issued device, MDM or EMM utility could put the EWSHS's network data and IT assets at risk, may result in the termination of an employee's use of an agency-issued mobile device(s) as determined by the Executive Director, and may result in other disciplinary action.
h. Agency-issued devices must comply with EWSHS Mobile Device Security Standards.
i. **Employees must immediately report the loss or theft of any mobile device used to conduct agency business.**
    I. Upon a report of loss or theft, EWSHS IT employees will immediately attempt to wipe agency-issued mobile devices via remote functionality, following established procedures.
    II. Agency-issued mobile devices must be configured to be remotely wiped when the maximum number of password attempts are made on the device, per OCIO Policy 141.10.

Article VI
USE OF EMPLOYEE-OWNED MOBILE DEVICES TO CONDUCT AGENCY BUSINESS

6.1 EWSHS employees who are authorized to use a state-owned device may request to alternatively use their personal mobile devices to conduct state business.

6.2 Prior to using an employee-owned mobile device to conduct agency business, the employee and Executive Director must complete a Mobile Device Authorization and Agreement form to document business need and policy acceptance. See Appendix A for the Mobile Device Authorization and Agrement.

6.3 EWSHS It employees will provide general instructions for employees with employee-owned mobile devices to set up their devices to receive email, calendar, etc. EWSHS IT employees are not able to provide troubleshooting or support for employee-owned mobile devices. The employee must obtain this support from their mobile provider.

6.4 The employee will be subject to the following:

a. Employee-owned mobile devices must be compatible with the EWSHS's MDM or EMM system. To use an employee-owned mobile device to conduct agency business, employees must enroll with and comply with the security settings of the EWSHS MDM or EMM system.
b. Tampering with the MDM or EMM utility could put EWSHS's network, data, and IT assets at risk and may result in the termination of an employee's authorization to use their

employee-owned mobile device to conduct agency business as determined by the Executive Director, and may result in other disciplinary action..

c. Employee-owned mobile devices shall not be used to conduct EWSHS official business or to access EWSHS records, only EWSHS email or other approved cloud-based containerized applications via the appropriate connections provided by EWSHS IT employees.
d. In accordance with the rulings from the Supreme Court of Washington, employees that use an employee-owned mobile device to conduct agency business are required to search for and provide any and all agency records created on the device pursuant to a public records request under chapter 42.56 RCW. Such employees may also be required to preserve, search for, and produce agency records on the device in response to a litigation hold.
e. EWSHS will maintain a process for employees to attest that they have searched for and provided any records located on employee-owned mobile devices that are responsive to public records requests or litigation.
f. The owner of an employee-owned mobile 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.
g. 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 records request.
h. Employees using an employee-owned mobile 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.
i. All call records, documents and date, photos, etc. used to conduct state business and made via employee-owned devices, are subject to state records retention requirements and the public records act.
j. If the device is lost or stolen, or the maximum number of password attempts are made on the device, the mobile device will be subject to being wiped remotely (State Security IT Standards) under the use of a Mobile Device Management system.

6.5 The EWSHS will manage an asset inventory of all approved employee-owned mobile devices.

6.6 Depending on budget constraints, the EWSHS may provide a stipend to partially offset the use of the employee-owned mobile devices. See BP#146 for further information.

Article VII
SECURITY, PRIVACY, AND RECORDS MANAGEMENT

7.1 Employees must follow state security standards and are prohibited from storing or relaying confidential information by such means unless authorized by agency policy. Additionally, mobile device activity and transmissions may not always be secure.

7.2 The State of Washington and the EWSHS reserve the right to monitor the use of all state-owned mobile devices and service. Employees should not expect privacy in their use of state-owned equipment and services.

7.3 Employees will not use text or direct messaging, to conduct state business. Any business-related decisions, transfer of agency files or communication of confidential information will be done through agency emails and not through text, direct messaging or voicemail. Texts and direct messaging will be considered transitory records and will not be retained by the agency.

7.4 Mobile devices used to conduct agency business will not be the primary storage location for agency data, per OCIO guidance on online file storage. Employees who create public records on their mobile devices shall remove those public records from their devices as soon as practicable after the records are created by either: (1) transferring the records to an agency file storage system for retention; or (2) deleting the records if deletion is permitted under the applicable records retention schedule.

7.5 All call records, documents, data, and photos, etc. used to conduct state business via an employee-owned device, and all contents of a state-owned device, are subject to records retention requirements and the public records act. Any personal call records or other information may also be subject to review or audit in the event in the event of a public records request or litigation hold. Personal data (data on a personal device that does not constitute a public record) is not subject to disclosure. However, all data on a state-owned device is deemed a public record.

7.6 The EWSHS is responsible for managing and retaining public records related to mobile device usage in accordance with records retention schedules, including but not limited to, billing and usage records.

7.7 The mobile device must be wiped remotely, by EWSHS IT employees, if the device is lost or stolen, or when the maximum number of password attempts are made on the device, per OCIO Standard 141.10, under the use of a Mobile Device Management system

Article VIII
AGENCY MANAGEMENT OF MOBILE DEVICES

8.1 The EWSHS is required to optimize the use of state-owned devices and service plans. Optimization may include one or more of the following:

a. Combining service plan subscriptions, where possible, within agencies to streamline billing and management and to enable statewide optimization.
b. Ensuring employees are using the most appropriate service plan by regularly monitoring and analyzing agency billing statements and usage reports to identify potential savings and efficiencies.
c. Working with mobile contractors and agency employees to identify and deactivate or reassign unnecessary cell devices.
d. Using the lowest cost method for long distance calls and related telecommunication services.

Article IX
EMPLOYEE RESPONSIBILITIES

9.1 Employees authorized to use state-owned or employee-owned mobile devices are responsible for:

a. Properly using the state-owned mobile device and equipment in their possession as required by state and agency policies.
b. Using the mobile device when it is the most cost-effective and efficient communication method compared to other tools (e.g. desk phones, SCAN long distance, or state calling cards).
c. Reviewing billing statements for accuracy as requested by the agency.
d. Ensuring employee-owned device records are retained in accordance with the EWSHS's records retention schedule.
e. Providing all relevant documents and communications stored on the mobile device if the EWSHS receives a public records request for records that may, in whole or in part, be within their possession.
f. Notifying their supervisor or EWSHS IT employees immediately in the event of damage, loss, or theft of mobile devices. The employee must provide written notification (email) within no less than three business days.
g. Complying, while on state business, with all laws applicable to the use of mobile devices while operating a motor vehicle, including RCW 46.61.672 (using a personal electronic device while driving).
h. Returning state-owned mobile devices to their supervisor immediately when they leave their position or are no longer authorized to use a mobile device for work purposes.
i. Obtaining technical support for their employee-owned mobile device from their mobile provider.
j. Complying with this policy when conducting state business using a state-owned or employee-owned mobile device to conduct state business.

References:

OCIO Policy 191	OCIO Standard 141.10
OCIO Guidance On Online File Storage	Chapter 42.52 RCW
RCW 42.56.010(3)	RCW 43.105.215
RCW 46.61.672	WAC 434-662-030

Appendix A – Mobile Device Authorization and Agreement

Business Need

Agencies must ensure state-owned mobile devices and service plans are necessary for business needs, and continue to improve the purchasing, assignment, and monitoring of mobile devices and service plans. The issuance of a state-owned mobile device, or the payment of a stipend, must be based on one or more the following job requirements:

☐ Employee's job requires field work or travel where landline phones are inaccessible or inefficient;
☐ Employee's job requires immediate or on-call availability;
☐ Employee needs a mobile device for work-related safety, security, or other emergency reasons;
☐ Employee's job requires real-time communication, including email; or
☐ Other requirements as defined and documented below by agency (and as agreed to by supervisor and employee):

_____
_____
_____

State-owned and/or Employee-owned Device Authorization

State-owned device: Yes _____ No _____
Employee-owned device: Yes _____ No _____

Authorized Stipend Amount and Plan

Type of access as needed by agency, and monthly stipend amount and service plan type (in lieu of state-owned device and plan):

☐ Voice access $10 / month
☐ Data access $30 / month
☐ Voice and data access $40 / month

Employee Signature:	Date:
Employee Position:	

By my signature, I agree to abide by all the conditions and responsibilities set forth in the EWSHS Mobile Device Policy, including the conditions for use of my personal device, to conduct state business. If my employer is issuing me a state-owned device or a stipend, I agree to have the cellular device available for the performance of my work responsibilities. This means the device must be in my possession and turned on during my assigned work hours to receive phone calls, access voice mail, and send and receive electronic mail. Specific details related to my availability during non-traditional hours will be determined by me and my supervisor based on the unique circumstances of my position. I understand and will comply with state and federal laws and all policy conditions and requirements as described in this policy, including, but not limited to:

- Records requests and records retention;
- All state and agency security policies and procedures, including the potential wiping of my device if lost or stolen, or too many attempted password attempts;
- Possible review or audit of my personal data and information;
- Possible device surrender if subject to public records request or litigation hold; and
- For authorized stipends, possible future imposition of payroll taxes, if required by law.

EWSHS Authorizing Signature:	Date:
EWSHS Authorizing Signature Position:	

By this signature, I acknowledge the following: The employee is authorized to use a mobile device for state business purposes as outlined above. I understand and agree to all policy conditions and requirements, including my agency and position responsibilities.