

Policy 1.1.8

Use of Mobile Communication Devices

Contact: Chief Legal Services Officer

1.1.8.1 Purpose

The Consolidated Technology Services (WaTech/CTS) Agency recognizes that for certain job functions it is critical that an employee be accessible when away from the assigned work location, during times outside scheduled working hours, or during times of emergency. For this reason, WaTech/CTS may provide a mobile communication device to select employees, or allow certain employees to connect to the State Shared E-mail Services via their personal mobile device. While acknowledging this need for communications, WaTech/CTS remains attuned to the costs associated with providing this technology and will be deliberate about its use.

This policy establishes criteria for determining the need for mobile communication devices and the requirements for their use.

Washington Technology Solutions (WaTech) refers to the “consolidated technology services (CTS) agency” identified in RCW 43.105.

1.1.8.2 Definitions

Mobile Communication Device(s) means any device that is capable of using the services provided by the public/private cellular networks. These devices can include pagers, simple cell phones, personal digital assistants (PDAs), or devices with the capability to access the Internet (“smartphones”, iPads, or tablets), Palms, game consoles, and handheld computers. A Mobile Communication Device can either be Employee Owned or WaTech/CTS Provided.

State Owned Confidential Information means all information exempt from disclosure under state law. If an employee is unsure as to whether information is confidential, the employee should contact the WaTech/CTS Public Disclosure Officer.

State Owned Sensitive Information means discloseable information that WaTech/CTS deems sensitive in nature and merits limited access.

Employee Owned Mobile Communication Device means a personal mobile communication device paid for by the employee but used for employer purposes.

WaTech/CTS Provided Mobile Communication Device means a mobile communication device provided to the employee by the employer.

1.1.8.3 Risk Statement

The improper or illegal use of mobile communication devices may result in serious risk and liability to both WaTech/CTS and the individual employee. These risks include but are not limited to:

- Loss of public trust in WaTech/CTS and state government

- Discovery violation and potential litigation sanctions
- Interference with performance and services
- Loss of network or operational integrity
- Financial loss
- Personal and agency liability

Employees are on notice that the use of any mobile communication device may result in the creation and dissemination of records that are not private, that are subject to monitoring, and that may be subject to disclosure pursuant to public records laws or discovery requests.

1.1.8.4 Appointing Authorities Determine Need and Appropriate Device Options

WaTech/CTS Appointing Authorities will review the need for State Provided Mobile Communication Devices and voice and data plans, then select the most appropriate and cost-effective solutions for their employees. WaTech/CTS Appointing Authorities will also review individual requests for using an Employee Owned Mobile Communication Device for conducting State business. The criteria to be considered in making the determination can be found in the [Mobile Device Decision Tree](#).

1.1.8.5 WaTech/CTS Provided Mobile Devices

Business Use and Requirement to Comply with Use of State Resources Policy

WaTech/CTS Provided Mobile Communication Devices are provided to employees as productivity tools for conducting state business. Employees are required to use such devices in performing their official duties. Employees' use of the same must be conducted in a manner that is consistent with public service and trust, all state and federal laws, State Ethics Law, WaTech/CTS Policy 1.1.4 (Use of State Resources) and WaTech/CTS Policy 1.1.7 (Use of Email and Electronic Communications Resources).

No Expectation of Privacy

Any user of a WaTech/CTS Provided Mobile Communication Device should be aware that any information placed in the system is subject to monitoring and is not subject to any expectation of privacy.

In order to ensure appropriate use of State Resources, including compliance with public records and records retention statutes, WaTech/CTS has the right to access, inspect, and/or monitor any State Resource. Because WaTech/CTS Provided Mobile Communication Devices are State Resources, WaTech/CTS is not required to provide notification to or seek permission from employees or other individuals using same prior to accessing, inspecting, and/or monitoring use.

If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of WaTech/CTS Provided Mobile Communication Devices are subject to appropriate disciplinary action.

Nothing in this policy shall be construed to give employees access to databases or systems that they are not otherwise authorized to access.

1.1.8.6 Employee Owned Mobile Devices

Must Comply with the Terms of the Personal Mobile Device Access Request Form

To ensure the security and integrity of the State's resources, it is imperative that employees who are approved to connect their Employee Owned Mobile Communication Devices to the State Shared Email Service complete and sign the Personal Mobile Device Access Request Form and comply with the requirements therein. A request form is required for the initial personal device and for each time the device is changed. If a device is replaced, the old device must be terminated and a new request form must be completed for the new device. Additionally, the employee must agree to abide by all applicable state and federal law and WaTech/CTS Policy 1.1.7 and OCIO Policy 191.).

Privacy and Employee Owned Mobile Communications Devices

Business related data created on Employee Owned Mobile Communication Devices should be saved and stored on the agency's secure infrastructure, not on the Employee Owned Mobile Communication Device. Information such as files, documents, and other data created, received or stored in connection with the transaction of WaTech/CTS business is subject to the existing records retention schedules and public disclosure laws as determined by content. WaTech/CTS reserves the right to access information stored on an Employee Owned Mobile Communication Device with proper notice.

Information on Employee Owned Mobile Communication Devices is private with the following exceptions:

1. When notified of a litigation hold, the employee may be required to consent to the inspection and copying by WaTech/CTS of data and electronically stored information as determined by the scope of the litigation hold.
2. When records are created and/or have been saved/stored on the Employee Owned Mobile Communication Device, the Device is subject to the requirements of public disclosure and records retention requirements.

Please note that in certain situations an Employee Owned Mobile Communications Device may have its data wiped in accordance with the Personal Mobile Device Access Request Form.

Stipends for Use: Employee Owned Mobile Communication Devices

WaTech/CTS authorize a monthly stipend for employees who use a personal cellular device in lieu of a State Provided Mobile Communication Device consistent with Office of the Chief Information Officer (OCIO) Policy 191. Authorization is allowed only when an employee is required to use a cellular device for the conduct of state business based on job requirements as follows:

1. The Employee's job requires field work or travel where landline phones are inaccessible or inefficient;
2. Employee's job requires immediate or on-call availability;
3. Employee needs a cellular device for work-related safety, security or other emergency reasons;'
4. Employee's job requires real-time communication, including email; or
5. Other requirements as required and documented by WaTech/CTS.

Employees must complete and obtain an approval Personal Mobile Device Access Request Form prior to receipt of a stipend. Employees receiving a stipend are responsible to:

1. Purchase the right device, service plan and coverage, to meet the agency's business needs;
2. Pay 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;
3. Receive and pay invoices directly for the Personal Mobile Device, WaTech/CTS is not responsible for the employee's cellular device or service plan;
4. Make their Personal Mobile Device phone number available to agency employees and constituents for the purpose of contacting the employee during their regular working business hours no later than five business days after approval of the stipend or activation of the service plan, whichever comes first.

Monthly stipends are as follows:

- | | |
|--------------------------|--------------|
| 1. Voice access | \$10 / month |
| 2. Data access | \$30 / month |
| 3. Voice and data access | \$40 / month |

All stipends will be paid through a payroll transaction. 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. WaTech/CTS will not provide a stipend as a replacement for amounts previously treated as wages.

WaTech/CTS will cease paying any stipend, when the first of the following events occurs:

1. Employee termination.
2. Agency ceases to have a business need for employee cellular access ; or
3. WaTech/CTS makes a decision to terminate the stipend for any other reason at the discretion of WaTech/CTS or employee.

1.1.8.7 Treatment of State Owned Confidential/Sensitive Information

Employees may access Stated Owned Confidential or Sensitive Information while using a Mobile Communication Device.

Employees agree to hold all such confidential or sensitive information in strictest confidence in accordance with all applicable laws and policies and in the same manner as if accessed from their WaTech/CTS office. Employees shall not use any confidential or sensitive information for any purpose other than as required by WaTech/CTS.

State Owned Confidential or Sensitive information shall not be stored on Employee Owned Mobile Communication Devices except for certain cases agreed upon with the supervisor. Where these cases apply, the data must be encrypted using approved encryption techniques and must be completely removed before separating from WaTech/CTS employment.

Employees agree to implement whatever safeguard is necessary to prevent unauthorized access to State Owned confidential or sensitive information.

1.1.8.8 Reporting Misuse

Employees who discover misuse of WaTech/CTS Mobile Communication Devices shall immediately report such misuse to their supervisors. It is not a violation of this policy for WaTech/CTS employees to forward Electronic Communication and Electronic Communication content to their managers, supervisors, and other individuals to report misuse.

1.1.8.9 Violation Warning

Violations of this policy may result in agency disciplinary action up to and including dismissal and other legal action. In addition, there may also be separate actions against the employee, contractor, or other involved party for violation of the state's ethics law, criminal code, or other law.

1.1.8.10 Policy Review

WaTech/CTS will review this Policy at least annually to assure it is consistent with any changes in markets, technology or legal requirements.

References

- [WaTech/CTS Procedure 1.1.8 - Personal Mobile Device Access Request](#)
- [Wireless Device Decision Tree](#)
- [RCW 40.14 et seq. - Preservation and Destruction of Public Records](#)
- [RCW 42.56 et seq. - Public Records Act](#)
- [WAC 292-110-010](#)
- [General Records Retention Schedules](#)
- [Executive Ethics Board](#)

Posted and effective: April 12, 2012

Revised: July 1, 2015

Sunset Review Date: July 1, 2016

Approved By:



Director
