




# OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY

## Information Services Division

|                        |  |  |
|------------------------|--|--|
| <b>Title:</b>          | <b>Bring Your Own Device</b>   | <b>ISD_610_02</b>  |
| <b>Supersedes:</b>     | None   |  |
| <b>Applicability:</b>  | State employees (and their agents)   |  |
| <b>Reference:</b>      | ISD_610_01 Acceptable Use of State Information Assets<br>ISD_620_01 Information Asset Classification |  |
| <b>Effective Date:</b> | <b>December 1, 2014</b>  | <b>Approved:</b><br> |

### I. PURPOSE

This policy establishes the expectations on the use of personally owned electronic devices (*aka: personal devices*) that are connected to the ODFW private network, systems, or devices. Other uses of personal devices within the workplace are also described.

### II. DEFINITIONS

A. **Connected Device:** Any connection using a wire, USB, Wi-Fi, Bluetooth, light wave, acoustic, cellular, radio wave, other means of syncing data between two or more devices.

B. **Employee (and their agents):** Employed by ODFW or a volunteer conducting business as an agent of ODFW. Excludes all other state employees, contractors, vendors, or guests of the agency.

C. **Information Asset:** Any data, application, computer, peripheral, portable device or other technology used to store, transport, modify, display, or report information that has value to the organization regardless of its physical form or characteristics.

D. **Personally Owned Electronic Device (aka: personal device):** Any computing device that is the property and responsibility of the employee (or their agent). Does not include agency owned devices.

E. **Public Network:** Public network in this policy refers to the portion of the network configured by ODFW that allows general public access.

F. **Private Network:** Private network in this policy refers to the network established and maintained by ODFW for its employees to conduct agency business.

G. **Stand Alone:** Any device can operate independently without a direct connection to agency systems or resources to perform a function. May or may not have the capability to transfer data or other information indirectly to other systems. (e.g. GPS, video or music player, cell phone).

H. **State Information Assets:** Any physical device, data, or knowledge that is acquired on behalf of the agency or while conducting agency business.

### III. POLICY

This policy is separated into distinct sections to clearly represent how the agency is implementing a Bring Your Own Device (BYOD) policy. Section 'A' describes limitations of connecting personal devices to the agency private network, systems and computing devices. Section 'B' describes allowable use of personal devices in a standalone mode or connected to the agency public network.

Caution: Employees must be aware and understand the difference between the agency's private network (restricted to ODFW devices only) and the public network for use by the general public.

#### A. Agency Private Networks and Computing Devices

##### 1. Applicability

Personal devices may be connected to an agency private network, systems or other devices **only when** a strong business case has been demonstrated and approved by the employees' manager, the form attached to this policy has been submitted to the Information Systems Division, and written approval has been granted.

An updated request form must be submitted anytime an existing electronic device is replaced with a new model.

##### 2. Information Security

Only information with classification Level 1 'Published' may be accessed without limitations. Data owners must explicitly indicate any Level 2 'Limited' information that can be accessed (if any) by personal devices. Access to information on personal devices with classifications of Level 3 'Restricted' or Level 4 'Critical' is explicitly NOT allowed under any conditions.

Please see policy ISD\_620\_01 'Information Asset Classification' for more information on data classifications.

##### 3. Access Authentication

Maintaining good security for mobile devices is essential considering they are easily misplaced, stolen, or accessed inappropriately. At a minimum, any personal electronic device in use under this policy must have password/passcode authentication to prevent incidental or intentional misuse.

4. **Maintenance and Updates**

Personal devices are expected to be maintained in good operating condition with current updates to the device and any applications it may contain. The agency at its discretion may provide or require the employee to purchase certain security applications.

5. **Information Transfer**

Information transferred to, or accessed from any personal devices remains the sole property of the state with all rights to restrict, delete, modify, or destroy to protect the security or sensitivity of the information or configurations.

Employee's personal information must not be transferred, stored, or duplicated to state systems for any purpose except to aid in maintaining a work schedule calendar or otherwise permitted by policy.

6. **Lost or stolen devices**

Employees will immediately report any lost or stolen personal electronic device that has direct access to state systems or contains agency data assets. Working with the employee, the agency will consider any risks and take any necessary actions to protect the privacy of the employee and agency and to maintain integrity of the lost device, up to and including a remote wipe of the device.

7. **Lifecycle**

There is no expressed or implied requirement for lifecycle replacements of personal devices. However, it is the expectation all devices are maintained in good working order and updated to meet minimum operating standards of the agency. The agency at its sole discretion may disallow devices deemed unfit or risky to operations at any time.

8. **Separation of Employment**

At the time of separation of employment, the employee must allow the agency the opportunity to review and/or purge any state/agency specific information from the personal device(s) previously allowed to connect to agency systems. This review includes, but not limited to, any data, software, configurations, or access privileges that may have been allowed by policy (if any). As necessary, may require a full factory reset of the device prior to returning it to the employee.

B. **Public Networks, Internet Accessible Services, Stand-Alone Devices**

The use of personal devices described in this section may have additional considerations such as when a device may be used, information classification, or if approval is necessary to conduct work outside normal business hours. Check with your supervisor.

See policy ISD\_610\_01 'Acceptable Use of State Information Assets' for additional information.

1. **Public Internet**

ODFW employees may bring their own personal devices to connect with agency's public Internet where available by office location. Such use must not interfere with agency business, work performance, or work schedules. Management may curtail use of the public Internet by employees use during special events or due to bandwidth limitations without notice.

Any personal use of the public internet by ODFW employees must comply with the provisions in policy ISD\_610\_01 'Acceptable Use of State Information Assets'. For example, an ODFW employee may use their own personal devices to connect to the agency's public Internet only during breaks or lunch periods but not before or after scheduled work time; it must be incidental and respectful of coworkers.

2. **Internet Accessible Systems and Services**

Personal devices may be used to remotely access agency systems and services that are designed to be accessible through any public or home Internet connection and does not require additional security services such as VPN (Virtual Private Network).

Examples of agency systems that can be accessed with personal devices include but not limited to Mallard (Web Outlook), iPOS control center, Snipe (External File Sharing) and similar applications.

3. **Lost or Stolen Devices**

Personal devices that are lost or stolen and have been used to access agency system or services that requires a password (such as Mallard) must immediately change their agency password(s) to prevent any potential unauthorized use. If assistance is necessary, contact the Information System Division.

4. **Stand-Alone Devices**

Personal devices may be used in the course of approved State business in a stand-alone operation if authorized by the immediate supervisor. Any such use of personal devices must not introduce risk to the agency or limit agency activities if the personal device is unexpectedly not available for the intended use(s) (e.g. left home for the day, in use by others in the family, lost, reconfigured, and faulty). The agency assumes no liability for wear, damage or loss of personal devices. An example might be a personal GPS device used for mapping stream coordinates.

5. **USB Storage Device**

Personally owned memory devices may be connected to agency computers only for the purposes of transferring agency information assets (data) and only when the memory device is connected directly to the computer's USB port, USB card reader, or otherwise connects as a USB portable storage device.

Use of any personally owned memory device with agency systems must be incidental and only when an agency owned device is not practical or readily available

Use of any personally owned memory device is limited to information with classification Level 1 'Published'.

Note: Agency owned USB memory devices should be used only for conducting agency business and not for personal use.

6. **Technical Support**

Employees are responsible for configuring and supporting personal devices. Limited technical support to assist with normal setup or configuration may be offered. Not all devices will be supported.

C. **Procedure**

Prior to using a personal device that connects to any agency private network or computing services, complete Attachment A 'Information Systems Certification Form' and submit for approval.

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technology and falls under the principle policy ISD\_610\_01 'Acceptable Use of Information Systems'.

## ODFW - Bring Your Own Device

This form is used to request authorization to use your personally owned electronic device in some form of direct connection (wired or wireless) with an ODFW computer, network, application, or other system. Pre-approval is required prior to any use. See additional information on ISD Inside for any specific limitations, details, or instructions prior to submitting this form.

### REQUESTOR INFORMATION

|                        |  |                                    |                       |
|------------------------|--|------------------------------------|-----------------------|
| <b>Employee Name</b>   |  | <b>State Employee Number (EIN)</b> | (Ex. OR0012345)<br>OR |
| <b>Supervisor Name</b> |  | <b>Division/Work Location</b>      |                       |

### DEVICE & REQUEST INFORMATION

**Device Type:**

|                          |                 |                        |  |
|--------------------------|-----------------|------------------------|--|
| <input type="checkbox"/> | Smartphone      | <b>Device Brand:</b>   |  |
| <input type="checkbox"/> | Tablet          |                        |  |
| <input type="checkbox"/> | Laptop          | <b>Device Model #:</b> |  |
| <input type="checkbox"/> | Other, Specify: |                        |  |

|   |  |
|---|--|
| <b>Business Purpose:</b>                  |  |
| <i>Please be specific</i>                 |  |
| <b>Device will be used to connect to:</b> |  |
| <b>Additional Notes:</b>                  |  |

### SIGNATURES & FORM DISTRIBUTION

*Employee's signature confirms s/he has fully read ISD Policy 610\_02, understands all personal liability, and has had the opportunity to ask any technical or policy questions with their manager and Information System Division.*

|                           |             |
|---------------------------|-------------|
|                           |             |
| <i>Employee Signature</i> | <i>Date</i> |

*Manager signature confirms approval of the user request and has discussed the policy and expectations with the employee. After approval forward this form to Information Systems Division for final approval.*

|                                     |             |
|-------------------------------------|-------------|
|                                     |             |
| <i>Manager/Supervisor Signature</i> | <i>Date</i> |

|                          |                 |   |                             |
|--------------------------|-----------------|---|-----------------------------|
| <input type="checkbox"/> | <b>Approved</b> | <b>Expiration/Review Period:</b>          | <i>Not to exceed 1-year</i> |
| <input type="checkbox"/> | <b>Denied</b>   | <b>If denied, ISD to state reason(s):</b> |                             |

*ISD signature authorizes use of personal device as described on this form and as allowed by ISD Policy 610\_02.*

|                                     |             |
|-------------------------------------|-------------|
|                                     |             |
| <i>Information Systems Division</i> | <i>Date</i> |

**Form Distribution:**

- Original to Employee
- Copy to Manager

- *Copy retained in ISD*
- *Copy to Employee's official personnel file*