OREGON DEPARTMENT OF FISH AND WILDLIFE POLICY
Information Services Division

Title:	Bring Your Own Device	ISD_610_02
Supersedes:	ISD_610_02 Bring Your Own Device dated March 1, 2020	
Applicability:	State employees (and their agents)	
Reference:	ISD_610_01 Acceptable Use of State Information Assets ISD_620_01 Information Asset Classification State policy 50-050-01 Working remotely	
Effective Date:	Jan 1, 2024	**Approved:** 

I. PURPOSE

This policy establishes the expectations on the use of personally owned electronic devices (***aka: personal devices***) that are connected to Oregon Department of Fish and Wildlife (ODFW) networks, systems, or devices. Other general use of personal devices within the workplace are also described.

II. DEFINITIONS

A. **Connected/Connection/Connecting:** Two or more devices that share or communicate using a wire, USB, Wi-Fi, Bluetooth, light wave, acoustic, cellular, radio wave, other means of syncing data between devices**.**

B. **Employee (and their agents):** Employed by ODFW or a volunteer conducting business as an agent of ODFW.

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 of the employee (or their agent) or otherwise not an asset of the agency.

E. **Public Internet:** The isolated portion of the agency network configured to allow public access to basic connectivity or agency resources.

F. **Stand Alone:** Any device that 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).

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

III. POLICY

The use of any personally owned devices for work-related functions or otherwise connecting, accessing, or interfacing with agency resources is not permitted for any purpose except as specifically allowed by policy. This is inclusive of all personally owned electronic devices.

A. Applicability

Per state policy, employees will not conduct state business on personally owned devices including cell phones, computers, laptops, or other information-storing devices (Re: Section 7(b) State policy 05.050.01 – "Working Remotely" and further clarified by memorandum by the Division of Administrative Service (DAS) director and state CIO titled "Use of Personal Devices and Statewide Policy 05.050.01 – working Remotely").

B. Cell Phones

The use of personally owned cell phones for agency use is prohibited by state policy. It is important to recognize that any records generated in conducting state business would be subject to public records law, any related public records requests, or associated retention requirements. Furthermore, in the event of litigation, the personal device would be subject to discovery and a potential legal hold.

Incidental use of a personally owned cell phone to communicate (call or text) to their supervisor of a late arrival, unavailability for the day, or urgent safety concern is acceptable however the call should be to the supervisor's work device to create an official record of the event.

C. Computers

The use of personal owned computers, tablets, or smart devices for agency use is prohibited. No exceptions are allowed per state policy.

D. Printers and Scanners

The use of personal owned printers or scanners for agency use is prohibited. No exceptions are allowed per state policy.

E. USB Storage Devices

The use of personally owned USB storage devices is prohibited for business purposes to store or transfer state data assets. No exceptions are allowed per state policy.

F. **Multi Factor Authentication (MFA) tokens**

Agency issued MFA tokens may not be used on personally owned devices for any purpose. This includes the use of soft (application based) or hard tokens (physical device). No exceptions are allowed per state policy.

G. **Virtual Desktop Infrastructure (VDI):**

The use of personally owned computers or devices to establish a virtual remote connection to agency cloud or on-premises hosted applications is prohibited. No exceptions are allowed per state policy.

H. **Application Software**

The use of personally owned software on agency devices is prohibited. Licensing violations could result in audit citations, fines, or criminal prosecution against the agency or employee. In addition, misconfigured settings or outdated patch management on personally owned devices could represent a security risk to agency information assets. No exceptions are allowed per state policy.

I. **Accessory Devices**

The use of any personally owned accessories with agency computers or devices is prohibited. Such devices may cause damage due to inferior quality or do not comply with industry standards. Examples include, but not limited to card readers, fans, toys, controllers, lights, scanners, etc.

J. **Personal Use Exceptions**

1. **WorkDay**

Employees can use a personal device to access WorkDay for non-work-related purposes (i.e. pay stubs, job applications). When performing any work functions in WorkDay a State issued device must be utilized.

2. **State Systems That Are Internet Accessible**

Personally owned devices may be used to remotely access agency and state-wide systems and services that have been established for personal or public use.

Examples of systems or systems that can be accessed with personal devices include but not limited to WorkDay, PEBB, PERS, and web applications available to the general public such as the ODFW and Oregon.gov public web sites.

3. **Peripherals**

The use of personal owned keyboards, mice, and monitors are allowed for use with agency computers and devices to accommodate the work at home environment.

The use of any personally owned peripherals that store or process information are not permitted per state policy.

4. **Public Wi-Fi**

Personally owned devices may connect with agency's **public** Wi-Fi Internet where available by office location. Such use must not interfere with agency business, work performance, or work schedules.

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, and is incidental and respectful of coworkers.

Management may curtail employee use of the public Wi-Fi during special events, security purposes, or due to bandwidth limitations without notice.

K. **Information Ownership and Rights**

Information transferred to or 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.

Employees' 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.

L. **Lifecycle**

It is the expectation all personal devices allowed for use are maintained in good working order and updated to meet minimum operating standards of the agency. The agency at its sole discretion may disallow personal devices deemed unfit or risky to operations even if otherwise permitted by policy.

M. **Technical Support**

Employees are responsible for configuring and supporting their own personal devices even when use is allowed by policy. Not all personal devices may function within an enterprise level environment. There should be no expectation of agency technical support for personal devices.

N. **Liability**

The agency assumes no liability for wear, damage, degradation, theft, or loss of personal devices under any circumstances. Employees should have no expectation of reimbursement or compensation related to any use.

O. **Procedure**

Prior to using a personal device for any purposes not specifically detailed in policy, an exception must be requested and approved by the ISD administrator or deputy. Exception requests can be submitted through the department's service request system (Service Desk+).

IV. Policy Group

This policy is part of a suite of Information Technology policies that collectively sets the expectations and use of computing devices and related technologies under the main policy ISD_610_01 'Acceptable Use of Information Systems'.