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 December 1, 2014	
Applicability:	State employees (and their agents)	
Reference:	ISD_610_01 Acceptable Use of State Information Assets ISD_620_01 Information Asset Classification	
Effective Date:	**March1, 2020**	**Approved:** Erica Kleiner

I. PURPOSE

This policy establishes the expectations on the use of personally owned electronic devices (***aka: personal devices***) that are connected to 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. **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 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).

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

The use of personally owned devices for work-related functions or otherwise accessing agency resources is not permitted except as specified by policy. This policy includes but is not limited to personally owned computers, tablets, phones, peripherals, GPS, locators, scanners, and other electronics.

This policy is separated into sections (work related and non-work related) to represent how the agency is implementing a Bring Your Own Device (BYOD) policy.

There is no expectation personal use will be reimbursed or compensated in any form. The agency assumes no liability for wear, damage, degradation, theft, or loss of personal devices.

A. Agency Networks and Computing Devices – Work Related Duties

1. Applicability

Connecting personal devices to an agency private network, systems, or other devices is not allowed unless provided specifically within policy. Exceptions may be considered **only when** a strong business case has been demonstrated and approved by the Information Systems Division Administrator or deputy. The use of agency owned devices is highly preferred to best manage information security and data integrity of the agency assets and resources.

2. USB Storage Device

Use of any personally owned memory device must be incidental and only when an agency owned device is not practical or readily available. Personally owned memory devices may be connected to agency computers only for the purposes of transferring data files 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 is limited to information with classification Level 1 'Published'. Data owners must explicitly indicate any Level 2 'Limited' information that can be accessed (if any) by personal devices.

See policy ISD_620_01 'Information Asset Classification' for more information on data classifications.

Note: Agency owned USB memory devices should be used ONLY for conducting agency business and never for personal use.

3. Smart Phone

Directly connecting personally owned smart phones (typically USB) to transfer data with agency information assets is not permitted.

4. **Accessory Devices**

Use of any personally owned accessories (typically USB) with agency information assets are not permitted. Examples include, but not limited to, card readers, fans, toys, controllers, lights, scanners, etc.

5. **Access Authentication**

At a minimum, any personal electronic device allowed under this policy must have password/passcode authentication that meets or exceeds agency standards to prevent incidental or intentional misuse.

6. **Maintenance and Updates**

Personal devices allowed under this policy 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 install or purchase certain security applications or licenses.

7. **Lifecycle**

It is the expectation all personal 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 personal devices deemed unfit or risky to operations.

8. **Information Transfer**

Agency 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.

9. **Lost or Stolen Devices**

Employees will immediately report any lost or stolen personal electronic device that has been authorized direct access to state systems or contains agency data assets. The agency will assess any risks and take any necessary actions to protect information up to and including a remote wipe of the device.

10. **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 direct access 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, this may require a full factory reset of the device prior to returning it to the employee.

B. **Remote Access – Work Related Duties**

Remote access is for business use only and requires prior approval by the supervising manager and any use must otherwise comply with agency policy. See policy HR_450_06 'Telecommuting and Teleworking' regarding alternate worksite requirements.

1. **Information Security**

Only information with classification Level 1 'Published' may be accessed with personal devices 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 unless such access is for the employees own personal employment, payroll or timekeeping access as allowed by agency practice.

Please see policy ISD_620_01 'Information Asset Classification' for more information on data classifications.

2. **Internet Accessible Systems and Services**

Personal devices may be used to remotely access only those agency and state-wide systems and services that have been approved for use by the entire agency.

Examples of systems or systems that can be accessed with personal devices include but not limited to Work Day, ePayroll, Mallard (Web Outlook), Snipe (FTP - External File Transfer), and web applications available to the general public.

Personal devices may not be used to remotely access systems or services that provide specialized, limited, or restricted access to perform systems administration or has access to restricted information.

Examples of systems or systems that cannot be accessed with personal devices include, but not limited to, ELS admin, network, security, or access systems consoles.

3. **Lost or Stolen Devices**

Personal devices that are lost or stolen and have been used to access agency systems or services (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. **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. **Work at Home – Work Related Duties**

In addition to the elements of section B 'Remote Access - Work Related Duties' the following is applicable when working at home:

1. **Peripherals**

The use of personal owned keyboards, monitors, and printers are allowed for work at home. The use of any additional peripherals especially those that store or process information requires prior approval to avoid potential security or device conflicts that could interfere with normal business functions. ODFW does not provide technical support for personally owned peripherals.

D. Stand Alone Use – Work Related Duties

Personal devices may be used in the course of approved State business that function fully in a stand-alone operation if authorized by the immediate supervisor. An example might be a personal GPS device used for mapping stream coordinates.

1. Operational Business Risk

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, or faulty).

E. Use of Agency Resources – Non-Work Related

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 employee 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, and is incidental and respectful of coworkers.

F. Procedure

Prior to using a personal device that connects to any agency private network or computing services except as allowed specifically in policy must compete the form 'Bring Your Own Device (BYOD)' and submit to ISD for approval. A copy of the form can be found under ISD Forms of the Resources section on the ISD Inside page.

BYOD approvals are not transferrable or reusable for similar circumstances. An updated request form must be submitted anytime an existing electronic device is added, upgraded, or replaced.

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 technology, and falls under the principle policy ISD_610_01 'Acceptable Use of Information Systems'.