ADMINISTRATIVE POLICY

SECTION: 600 – Information Technology	**POLICY#:** 602
TITLE: Information Technology Acceptable Use Policy	**R & O #:** 17-28
	IMPLEMENTED BY PROCEDURE #:
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 02/28/2017	**REVIEWED:** 11/4/2024

PURPOSE:

County-owned, third-party, or personal technology is used by Washington County ("County") workforce members to conduct County business. Using technology wisely means being thoughtful and respectful. This includes valuing the trust of the public, the broader online community, and the access privileges we've been given.

The use of technology imposes specific responsibilities and obligations on users and is subject to County policies and applicable local, state, and federal laws. Unacceptable use of technology can lead to negative consequences and cause service disruptions, malicious attacks, compromise of network systems and services, breach of confidentiality, and legal liability.

This policy is intended to provide workforce members with guidelines for responsible and appropriate use of technology within Washington County.

OBJECTIVES:

1) Ensure the confidentiality, integrity, and availability of County IT resources that may be utilized by the County or any of its Agents.
2) Ensure proper use of County IT resources.
3) Prevent access to County IT resources from unauthorized users or unauthorized access or unauthorized use.

4) Inform workforce members that there is no expectation of or right to privacy in their use of County IT resources.
5) Ensure County IT resources are used solely for authorized and appropriate purposes, avoiding personal gain or political activities.
6) Prevent individuals from wrongfully or improperly using or harming County IT resources.
7) Inform workforce members on the acceptable use of personally owned technology.
8) Ensure awareness that the use of information technology in the conduct of County business is subject to Oregon Government Standards and Practices Laws.
9) Ensure that the County maintains and stores all electronic information and communications created, processed, or stored in the conduct of County business in compliance with Oregon Public Records Laws and civil litigation.
10) Clarify data ownership and accountability.
11) Protect the County against legal issues and cyber-related security threats.

AUTHORITY:

This Policy will be administered by the County Administrative Office in accordance with Section 34 of the Washington County Charter and the authority delegated to the County Administrator in Washington County Code Section 2.04.100.

DEFINITIONS:

1) **Workforce Member**: All authorized personnel in the County that use information technology to support County business. This includes, but is not limited to, employees, contractors, consultants, temporary employees, volunteers, and interns.

2) **Stipend Program**: This program allows qualifying employees reasonable compensation for using a personal cell phone or Smart Phone for County business. Personal use limitations are removed from mobile communications devices subsidized under the stipend program. Still, ITS User Responsibility Policy guidelines continue to apply to the extent the device is used to access the Technology Environment.

3) **County Technology**: The County owns and controls the following information technology. This includes but is not limited to:

    a) All electronic networks (including internet connectivity), devices, and portable mass media either purchased, leased, administered, contracted, or subscribed through a third-party vendor or otherwise under the custody and control of the County.

b) Electronic information: Includes communications or data generated, processed, and/or stored for County business purposes or that impacts the County in any way regardless of the physical location of the data (including personally owned devices and Internet) or the means through which data is accessed.

c) Electronic Infrastructures and Networks (Voice and Data): Enterprise Data Networks (physical, wireless, voice, and VPN networks).

Connectivity services: Includes but are not limited to:

i) Microsoft 365 allows all workforce members with assigned email accounts access to County email and calendaring remotely through any browser-equipped Internet connection.

ii) Virtual Private Network (VPN) and remote-control solutions extend full capabilities to workforce members from outside the physical boundaries of the County enterprise network.

iii) Virtual Desktop Infrastructure (VDI) - utilizing the ITS-approved solution to access enterprise computer systems from almost any device, such as a personal device.

iv) Mobile Data Management (MDM) - To ensure security standards are met, only mobile devices provisioned through County ITS can sync with the county's Microsoft Office 365 environment.

d) Cloud-hosted computing resources are used to support county businesses.

4) **Personally Owned Technology** (Aka: BYOD or Personal Devices)**:** Any technology you own that is approved by your Department Director, but not managed by County IT, that is used to conduct County business. Includes but is not limited to your cell phone, laptop, computer, portable devices, applications, or email account.

APPLICABILITY:

This policy applies to:

1) All workforce members engaged by the county should use information technology in support of county business. This includes but is not limited to all authorized full-time equivalent individuals of any status (FTEs), contractors, consultants, temporary employees, volunteers, and interns.

2) All County-owned, third-party, or personal technology used in the conduct of County business.

GENERAL POLICY:

The County's policy is that technology is a resource and tool to assist in the efficient conduct of County business. Unless otherwise specified by the initial agreement, the use of any technology in support of County business shall be conducted in accordance with this policy.

The use of information technology for County business is not considered personal or private. The County has the right to access any county-issued information technology that stores county-related electronic information at any time, without the knowledge or consent of a workforce member.

This policy requires all workforce members to read and understand it annually.

POLICY GUIDELINES:

Responsibilities:

The following guidelines highlight many, but not all, of workforce members' expectations regarding technology use. Expectations that require more context are included in the annual Mandatory Security Awareness Training.

Workforce Member Responsibilities

1) Complete Mandatory Security Awareness Training (SAT).
    a) The SAT will be comprised of reading and understanding this Policy and may also include additional training material that pertains specifically to emerging threats that are highly likely to impact the County.
        i) All county workforce members must know how to use and protect technology. As such, ongoing Security Awareness training is required:
            (1) All new County workforce members must undergo County Security Awareness Training within 30 days of their first day of work.
            (2) All County workforce members must recertify annually within 30 days of the County's Security Awareness Training (SAT) enrollment notification.
            (3) Recertification requires, at minimum, all workforce members to read and understand this policy.
            (4) County workforce members who do not have a County email address but have access to the County network must prove to their hiring Department that they have completed Security Awareness Training by a certified external provider.

2) Ensure the confidentiality, integrity, and availability of County information that needs to be protected by reading and understanding the following policies:
    a) Policy 208 – Management, Preservation, and Storage of Electronic Public Records
    b) Policy 501 – HIPAA Privacy
    c) Policy 506 – Personal Information Protection
    d) Policy 601 – Texting, Microsoft Teams Chat
    e) Policy 606 – Cloud Services
    f) Policy 607 – Artificial Intelligence
    g) Policy 608 – Recording of Meetings
    h) Social Media Policy
3) In general Oregon Government Standards and Practices Laws prohibit any workforce member from using their official position as representatives of the County to obtain financial benefit or avoid financial detriment.
4) Bring Your Own Device (BYOD)/Personal Devices
    a) It must be approved for use by the Department Director and provisioned by ITS to securely connect to County-owned technology.
    b) ITS does not provide technology support for personal devices.
    c) It is advised that individuals keep their professional and personal technology separate if possible. Electronic information related to an individual's work is considered a public record. Use of a personal device or account may subject the entirety of an individual's device or account to disclosure in accordance with public records law or litigation.
5) Devices Connecting from Abroad
    a) Before traveling, obtain approval from the Department Director and notify ITS to confirm that the device is authorized to access County technology. Some locations may have restrictions.
6) Portable Devices and work environments must be secured to prevent unauthorized access to protected information.
7) Ensure that content/communications are delivered to the intended audience and are secured when required for regulatory compliance.

8) Software

   a) Software not owned or managed by County ITS can only be downloaded onto County-owned devices with the Department Director's and ITS approval.

   b) Only change software on County-owned devices if you have permission from ITS.

9) Personal Accounts

   a) Do not use personal accounts to conduct County business. Any exceptions to this rule should be approved by your Department Director.

10) Using County-Owned technology for Personal Reasons

   a) Do not do anything illegal.

   b) Do not do anything that results in a direct cost to the County.

   c) Do not use County technology in a way that interferes with your work duties.

   d) Do not engage in personal business, political activities, or profit-making ventures.

   e) Do not access sites containing pornographic or offensive materials.

Information Technology Services Responsibilities

1) Create, maintain, and distribute a comprehensive Acceptable Use Policy that outlines acceptable and unacceptable behaviors when using County technology.

2) Administer and track Annual Mandatory County Security Awareness Training compliance.

Elected Officials, Department Directors, and Managers

1) Are expected to be knowledgeable of, and shall be responsible for, implementing this policy within their respective departments.

2) Enforce compliance with this policy. Non-compliance can lead to disciplinary action as defined in the Washington County Personnel Rules and Regulations Policy.

3) Are responsible for establishing organizational practices to ensure compliance with data privacy and protection laws, regulations, and policies.

4) Report policy violations to ITS or Human Resources (HR).

Data Security Officers and Privacy Managers

1) Ensure that the applicable department regulatory security compliance requirements are addressed in organizational practices.
2) Ensure that workforce members know the requirement to complete the Incident and Risk Assessment form to report any suspicious use, experience, or technology-related incidents.

Public Records Officer

Ensure department workforce members know and practice Policy 208 - Management, Preservation, and Storage of Electronic Public Records.

Exceptions:

Exceptions may only be granted by the Washington County Board of Commissioners unless such authority has been delegated to the County Administrator.

Implementation:

Elected officials and department directors are expected to be knowledgeable of and responsible for implementing this policy within their respective departments. Observance of this policy is mandatory for all County employees, and violation may result in disciplinary action (up to and including termination).

Periodic Review:

This policy shall be reviewed by the Department of Information Technology Services at least every three years, or more often if needed, and updated as necessary.