UNIVERSITY OF OREGON FOUNDATION

Policy: Acceptable Use

Title: Acceptable Use	
Department: Information Technology	**Policy Owner**: VP of Technology Services
Effective Date: September 1, 2023	**Replaces Policy Dated**: June 21, 2016

PURPOSE:
To guide users in the acceptable use and exchange of Foundation data, computer systems, networks and other information technology resources. These rules are in place to protect the employee and the Foundation. Inappropriate use exposes the Foundation to risks, including virus attacks, compromise of network systems and services, and legal issues.

SCOPE:
The University of Oregon Foundation is committed to high standards of excellence for the use and protection of technology resources that support our mission. The Foundation receives, processes, stores, creates, and transmits an immense quantity of information to conduct its business functions as well as those business and stewardship functions of the University described in the Recognition and Relationship Agreement. These systems and networks are provided to support Foundation and University business. Appropriate controls and security measures are implemented to protect these assets from potential damage or compromise to confidentiality and to mitigate interruption to Foundation and University activities. Uses that threaten the integrity of the system, privacy or safety of others or are illegal are forbidden.

This policy applies to, but is not limited to, the use of information, electronic and computing devices, and network resources used to conduct business on behalf of the Foundation or interact with the Foundation internal networks and business systems. This includes all assets used to conduct business, whether owned or leased by the Foundation, the employee, or any third party. All employees, contractors, consultants, temporary, and other workers at the Foundation and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources per the Foundation's policies and standards, as well as local laws and regulations.

POLICY:
Foundation technology resources are provided to *authorized users* to support Foundation and University business. Users are expected to use computer and network resources in a responsible manner. Personal conduct prohibited by policy or law also applies to electronic forums, including but not limited to illegal discrimination and harassment, lewd or indecent conduct, threat of imminent physical harm and forgery.

Users should take appropriate precautions to ensure the security of their passwords and prevent others from obtaining access to their resources; sharing an account is prohibited. User access will be reviewed and renewed annually. Annual attendance at a security class that provides information on best practices and adherence to guidelines will be required.

All information on and produced from Foundation-owned technology, whether or not stated on a specific document or electronic form, should be treated as confidential, including but not limited to all information contained on the donor and financial databases of the Foundation known as "Advance", "Laserfiche" and "Financial Edge," respectively; all other data, materials, products,

technology, computer programs, specifications, manuals, business plans, software, financial information, and donor information; and other information that a reasonable person would understand should be treated as confidential information and that is disclosed or submitted, orally or in writing, or by any other media, by the Foundation. The Foundation's fiduciary responsibilities over donor's charitable activity includes protection of the expectation that donor information will be held in confidence. Any unauthorized reproduction, dissemination, or disclosure is prohibited.

In accordance with the Foundation's role as the University's appointed institutionally related foundation, the Foundation supplies confidential information and data, including donor information, to certain authorized University users. This information is provided only to those authorized users that demonstrate a specific business need for that information. It is understood that the exchange of any information that includes details of donor giving between Foundation and specific authorized University users is consistent with and maintains the donor's expectation of holding donor information in confidence; any further dissemination or use of that information is in breach of the donor expectation under which the giving information was originally provided.

Information generally available to an authorized user or provided by request is available only for their approved business need. Further release requires specific approval from the Foundation VP of Technology Services or as described:

- All requests from media sources must be authorized specifically by the Foundation President/CEO
- All requests as a result of a legal action or pursuant to a legal request must be authorized specifically by the Foundation President/CEO
- Requests for data to be provided to external vendors or contractors to meet business needs for the Foundation, UO Advancement or UOAA must be authorized by the VP of Technology Services after a review of all relevant contract language and provisions
- Any request, other than from the donor, for anonymous information or records must be approved by the Vice President of UO Advancement (or their designee).

It is expected that University users of any confidential information and data, including donor information, do not retain the information for a future use unrelated to the specific circumstances under which the information was shared. Further, all additions to or edits of this information (created work) shall be returned to the Foundation and not independently retained.

Any suspected or known compromise of data, including but not limited to, equipment loss, misplacement of sensitive documents, exposure of password, and installation of unauthorized software, must be promptly reported to the HelpDesk at helpdesk@uofoundation.org or 541-302-0338

Employee Responsibilities

All Foundation employees and contractors must maintain basic controls to prevent technology assets from being lost or stolen, potential security breaches, leaking of confidential information or personal information, and breaches of software licensing agreements.

The Foundation provides technology to be used for legitimate business purposes. The employee is expected to exercise good judgment and professionalism in the use of all technology. Incidental personal use is allowed, provided that, in addition to the constraints of this policy, such use does not interfere with the user's employment or other obligations to the Foundation. Any personal information passing through or stored on Foundation-owned technology is property of the Foundation and subject to all Foundation policies. The Foundation assumes no liability for loss of any personal data or communications transmitted or stored on

Foundation-owned technology.

Employees must maintain confidentiality and exclusive control of authentication credentials (passwords, tokens, certificates) used to access the Foundation's technology. Credentials must not be shared with others or left in a place where an unauthorized person might find them. If the employee has any reason to believe that their password has been compromised or discovered by another person, they must immediately inform the HelpDesk (helpdesk@uofoundation.org) and change their password immediately. Other basic controls include, but are not limited to:

1. Ensuring that laptops, mobile devices, and desktop computers are protected by lock screen passwords of at least 8 characters in length and that screens are set to lock within 10 minutes of inactivity.
2. Keeping laptops, mobile devices, portable storage devices, and media appropriately secured (e.g., not leaving these items unattended in a vehicle or public place).
3. Not sharing mobile devices used to access the Foundation's technology or portable media containing confidential information or assets with third parties (including family members).
4. The employee must exercise caution when opening attachments or selecting links (these can be contained in electronic messages, blogs, or social networks) from unknown sources. These may contain malicious software (also known as malware; examples include viruses, worms, and trojans).

All Foundation technology resources must be returned to the Foundation at the end of the employee's employment, or at any time the Foundation deems it necessary.

Unacceptable Use

Users may not encroach upon others' use of electronic resources. Examples include, but are not limited to, interference with or disruption of computer or network accounts or services, propagation of viruses, sending of electronic chain mail. Under no circumstances is an employee of the Foundation authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Foundation-owned resources. Examples include, but are not limited to the following:

1. Revealing account passwords to others or allowing others to use the account. This includes family and other household members when work is being done at home.
2. Using a Foundation computing asset to actively procure or transmit material that violates sexual harassment or hostile workplace laws in the user's local jurisdiction.
3. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Foundation.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Foundation or the end-user does not have an active license is strictly prohibited.

Authorized Access

While respecting users' privacy to the fullest extent possible, the Foundation reserves the right to examine any computer files or transmissions. The Foundation reserves this right for bona fide purposes, including, but not limited to:

- Enforcing Foundation policies, including those against harassment and threats to the safety of individuals
- Protecting against or limiting damage to Foundation technology resources, including authorized contracted vendors for audit, security and maintenance purposes

- Upgrading or maintaining technology resources
- Safeguarding the integrity of computers, networks, software and data
- Preserving information and data
- Other purposes deemed operationally necessary
- When required by law

The Foundation reserves the right to revoke access to or use of any organizational technology at any time at its sole discretion. Access to technology will be revoked when the employee leaves the Foundation.

ENFORCEMENT AND EXCEPTIONS
The Foundation may restrict the use of its computers and network systems when presented with evidence of violation of Foundation policies, or federal or state laws, or when it is necessary to do so to protect the Foundation against potential legal liability. The Foundation reserves the right to limit access to its information technology resources, and to remove or limit access to material stored on Foundation technology resources.

Unauthorized use of Foundation technology may result in loss of access rights and may subject the person to further disciplinary or legal action. Anyone who becomes aware of the occurrence of any violation of this policy should report the violation promptly to their supervisor or Foundation management.

The VP of Technology Services is authorized to grant exceptions to the requirements set forth in this policy. Exceptions must be submitted in writing and must include a detailed business case supporting the need for the exception. Any consideration of an exception will require a thorough review of the situation by Foundation Leadership. An approved exception will require the implementation of appropriate compensating controls.

REFERENCES:
NIST 800-53 Rev 5: PS-6

POLICY HISTORY

Version	Approved By	Date	Description
1.0	Brian Ikei, VP of Technology	11/28/2022	Updated policy from June 2016