University of Portland

ACCEPTABLE USE POLICY

1. **PURPOSE:** The purpose of this policy is to define the ethical and acceptable use of University of Portland technology resources and to outline user responsibilities and expectations for security and privacy.

2. **SCOPE:** This policy applies to all users of technology resources provided by the University of Portland, including students, faculty and staff.

3. **POLICY:** The University recognizes the importance of technology in fulfilling its mission for teaching and learning, faith and formation, and service and leadership. For this reason, the University provides a range of technological tools, including hardware, software, and connectivity, to students, faculty, and staff.

   a. **Acceptable Use:** This technology and access is a privilege granted to support the members of our community. These tools are shared by many people in the University community and provide the most benefit for everyone when they are used responsibly and respectfully.

      - **Institutional Purposes:** Faculty, staff, and students may use computing resources for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, and other University-sanctioned or authorized activities.
      - **Responsible Use:** All members of the University community who use the University's computing and information resources must assume responsibility for legal and ethical computer and network use including honest representation of identity and authorship. Responsible use encompasses respect for the rights of others including respecting privacy, using only authorized access, respecting intellectual property, respecting sensibilities of others, and not knowingly doing harm to or denying service to others.
      - **System Integrity & Safety:** Every user is responsible for the integrity of the computing resources. This applies to all devices connected to the campus network, including those in all campus buildings and facilities, and those using remote access connections. All data transmitted and received using University networks or which are stored on University systems are University records. The University does not purport to control the content of electronic materials, but it does make available procedures for reporting violations of University policy for the safety of the user.

   b. **Unacceptable Use:** Computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission of the University, or likely to subject the University to liability. Unacceptable uses include, but are not limited to:

      - Harassment by use of computing facilities, specifically by the use of messages or mailings that contain offensive or harassing language or the display or transmission of sexually explicit images, cartoons, jokes, or messages.
      - Violation of the privacy of others. Sensitive or confidential information regarding students or employees should not be discussed in any electronic media format.
      - Theft of or destruction or damage to equipment, software, or data/information belonging to the University or others.
      - Unauthorized use, alteration, or removal of computer hardware.
      - Disruption to or performing unauthorized monitoring of electronic communications.
      - Violation of computer system security.
      - Use, without authority, of computer accounts or access codes.

- Use of computing facilities for purposes contrary to the mission of the University.
- Violation of copyright and software license agreements.
- The download and/or distribution of copyright protected data without prior approval
- Academic dishonesty, such as plagiarism and scientific misconduct.
- Using University resources (power, compute, network, cooling) for personal gain. This can include the mining of cryptocurrency or other activities that may benefit the individual and harm the University.
- Misrepresenting one's identity in electronic communication.
- Using the University's trademarks, logos, insignia, or copyrights without prior approval from the Office of Public Relations.
- Using computer resources for any purpose that is likely to subject the University to liability.
- Commitment of crimes or prohibited acts. Illegal acts involving University computing facilities may also be referred to State and Federal authorities for prosecution. (Sermersheim, NACUA, 1998)
- Using computer resources in a way that is wasteful or unfairly monopolizes resources to the exclusion of others. This includes, but is not limited to, sending unauthorized mass mailings, initiating or facilitating electronic chain letters, creating unnecessary multiple jobs or processes, producing unnecessary or excessive amount of output or printing, or creating unnecessary network traffic.
- Use of University computing resources for unauthorized commercial purposes, including any sort of solicitation. Unauthorized commercial uses of University computing resources jeopardize the University's relationships with network service providers and computer equipment and software vendors.
- Recreational use to the extent that network performance is degraded, impacting network use for academic and administrative purposes.

c. **User Privileges and Responsibilities**: Access to computing resources is a privilege made available by the University. The University also makes available to the user appropriate training, support, documentation, and tools to affect that access. The primary use of University technology resources should be related to the person's educational, scholarly, research, service, operational, or management activities within the University. Use of University electronic systems will constitute awareness and acceptance of the responsibilities regarding the access and responsible and ethical use of these systems. The user is responsible for the activity connected with their assigned account(s) and assumes full legal and moral responsibility for the content. Electronic communication may not be represented as the views of the University.

d. **Security:** Electronic communications are by no means secure. Exercise caution when committing confidential information to electronic media given that the confidentiality and integrity of such material are difficult to ensure. The user is responsible for knowing and complying with all applicable laws, policies, and procedures. E-mail and user accounts and their contents are generally considered private by University of Portland, but neither this policy nor present technology can guarantee security, privacy or confidentiality. It is not the routine policy of IS administrators to view or disclose the content of others' electronic files, but University of Portland reserves the right, and may be legally required, to access, copy, examine, and/or disclose all files stored or transmitted on, across or through UP IS Resources, in several circumstances, including:

- for safety, security, and/or legal purposes;
- as needed to maintain or protect its personnel, facilities and not-for-profit status;
- as necessary to maintain network services;
- or in order to protect University of Portland rights or property. For these reasons, there should be no presumption of privacy or confidentiality concerning information stored on or transmitted across University of Portland Resources.

e. **Privacy and Confidentiality**: Data are institutional resources and must be protected from unauthorized change, destruction, or disclosure, whether accidental or intentional. Unauthorized sharing of University data to outside agencies or vendors is prohibited. The University complies with applicable laws and regulations regarding the dissemination and protection of confidential data. The University adheres to the Family Educational Rights and Privacy Act of 1974 ("FERPA"), also known as the Buckley Amendment, as well as the Health Insurance Portability and Accountability Act ("HIPAA"). Users should be mindful of the privacy rights of students under FERPA and ensure that all student records or any information related to a student be kept confidential.

4. **EXCEPTIONS:** The University provides access to a large variety of information, including from Internet sources. This information is not affiliated with, endorsed by, edited by, or reviewed by the University. The University takes no responsibility for the truth or accuracy of content of the information from these sources, and some of these sources may contain material that is objectionable or offensive. This policy is an addition to University rules and regulations published in the documents cited above, and does not alter or modify any existing University rule or regulation.

5. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.