

OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

890 ACCEPTABLE USE

SUBJECT: ACCEPTABLE USE

NUMBER: 890

AUTHORIZING BODY: PRESIDENT'S CABINET

RESPONSIBLE OFFICE: CHIEF OF STAFF

DATE ISSUED: JULY 2003

LAST UPDATE: FEBRUARY 2026

RATIONALE:

The use of Oakland University (University) Network and Information Resources should support the teaching, learning, clinical, and research missions of the University and their supporting administrative functions. The policy is intended to ensure:

- The security, integrity, availability, and performance of University resources;
- The user community operates according to established policies and applicable laws;
- These resources are used for their intended purposes; and
- Appropriate measures are in place to ensure the policy is honored.

POLICY:

Users of the University's Information Resources are expected to use resources properly and respect the rights of others. This policy addresses the authorized use of all Information Resources, including computers, networks, cloud services, social media, and data stored, processed, and transmitted.

To ensure Information Resources are used effectively and securely to further the University's Mission, each User has the responsibility to:

- Use the resources appropriately and efficiently.
- Respect freedom of thought, inquiry, and expression.
- Respect the privacy of others.

- Protect the stability and security of the resources.
- Understand and fully abide by the established Oakland University policies and applicable federal and state laws.

SCOPE AND APPLICABILITY:

This policy applies to all individuals who access, use or control Information Resources at the University, including faculty, staff, and students, as well as contractors, consultants, and other agents of the University and/or individuals authorized to access Information Resources by affiliated institutions and organizations.

DEFINITIONS:

- Capitalized terms used herein without definition are defined in the IT Terminology Standard.

PROCEDURES:

All of the following apply to use of the University's Information Resources:

1. Laws, policies, contracts, and licenses: Users must comply with all federal, state, and local laws, and regulations, University rules, policies and procedures, and contracts and licenses applicable to their use of Information Resources.
2. Authorized use/access: Access to Oakland's Information Resources is a privilege granted to faculty, staff, and students in support of their studies, instruction, duties as employees, official business with the University, and/or other University-sanctioned activities. Access may also be granted to individuals outside the University for purposes consistent with the University's mission.
3. Data security and privacy: University Users are responsible for understanding the various Data Classifications, ensuring the security and appropriate use of University Data to which they are given access, ensuring the security of the equipment where such information is held or displayed, ensuring the security of any accounts issued in their name, and abiding by related privacy rights of students, faculty, and staff.
4. Information Resource integrity and availability: Activities and behaviors that threaten the security, integrity, and availability of the University's Networks, Endpoints, and Systems are prohibited on University-owned and privately-owned equipment operated on or through University resources. Lost or stolen equipment must be reported immediately.

5. Commercial use and political campaigns or advocacy: Information Resources shall not be used for unauthorized commercial activities or political campaigns or advocacy.
6. Libel, slander, and harassment: Information Resources shall not be used to libel, slander, or unlawfully harass any other person.
7. Monitoring and Recording: The University may monitor, record, and audit use of the University's Information Resources (collectively "Monitoring and Recording"). By using Information Resources, Users consent to the Monitoring and Recording of such use. The results of Monitoring and Recording may be disclosed to appropriate University authorities and law enforcement agencies and used in disciplinary procedures.
8. Electronic communications: University electronic communications are to be used to enhance and facilitate teaching, learning, clinical, and research to support academic experiences, to facilitate the effective business and administrative processes of the University, and to foster effective communications within the academic community.
9. Generative Artificial Intelligence (GenAI): Users shall not input or process University Confidential or Internal data using AI systems that have not gone through the UTS IT Review Process.
10. Digital Millennium Copyright Act (DMCA): Oakland University adheres to the procedures outlined in the DMCA for responding to reports alleging copyright infringements on the University's Information Resources.

Sanctions:

- A. Use of the University's Information Resources is a privilege. A User's access to Information Resources may be limited, suspended, or terminated if the User violates this policy. Alleged violations of this policy will be addressed by the Information Security Office. If the Information Security Office determines that a User has violated this policy and limits, suspends, or terminates the User's access to Information Resources as a result, the User may appeal the decision to the Chief Information Officer who will facilitate review through IT Governance processes.
- B. Users who violate this policy may also be subject to disciplinary action and other penalties, up to and including dismissal from the University. Disciplinary action for violations of this policy will be referred to the appropriate departments and handled through the University's normal student and employee disciplinary procedures. Appeals of disciplinary action should be directed through established procedures for employees and students.

C. Some violations of this policy may constitute criminal offenses under federal, state, or other laws. The University will carry out its responsibilities to report such violations to law enforcement and other appropriate authorities.

RELATED POLICIES AND FORMS:

- Merit Network, Inc., operates the statewide network MichNet, which provides Internet access for the University. Merit is a non-profit corporation governed by all thirteen of Michigan's four-year publicly supported universities, including OU. University participation in MichNet and access to the Internet in general is governed by their Acceptable Use Policies.

APPENDIX: