OBERLIN
COLLEGE & CONSERVATORY

Acceptable Use Policy

Purpose

At Oberlin College and Conservatory ("Oberlin," "College"), we use technology for learning, teaching, and working. Our Acceptable Use Policy (AUP) ensures a positive and secure digital experience. It protects our network, data, and user privacy. By following the guidelines, we maintain a secure environment and promote respectful use of technology.

Scope

This Policy applies to individuals who directly, or through any agent acting on their behalf, interact with Oberlin College Technology Resources, regardless of affiliation or location.

Policy

General Use, Ownership, and Stewardship

Written consent, duly authorized by the college, is required for any deviations from this policy. All members of the Oberlin college community are required to immediately report any incidents of theft, loss, or unsanctioned exposure of confidential information.

Only authorized users can access, use, and share information as needed to fulfill their assigned responsibilities. It is their responsibility to exercise good judgment and ethical conduct when handling this data. Authorized users can seek clarification, additional guidelines, or answers to their questions by consulting their designated supervisor or manager, in addition to receiving specialized training.

Confidentiality of Data and Information

Confidential Data Handling Guidelines:

- **Non-Disclosure:** Confidential data must not be shared or disclosed to individuals not employees of Oberlin.
- **Internet and Public Systems:** Confidential data should not be posted on the Internet or any publicly accessible systems without proper authorization.
- **Secure Transfers:** Confidential data must always be transferred using secure and authorized methods to ensure its protection during transmission.

This is a summary of the guidelines for handling confidential data. More comprehensive policies provide detailed instructions on the proper use of such information. It is essential for all users to thoroughly understand all of Oberlin's IT and Cybersecurity policies, guidelines, and procedures.

Network Access

Oberlin College provides network access to its students, faculty, staff, and authorized guests to support education, research, and administrative activities. By accessing the network, users agree to abide by the following guidelines:

- **Authorized Use:** Users may access the network for legitimate academic, research, and administrative purposes related to Oberlin College. Any unauthorized use, including but not limited to activities that violate local, state, or federal laws, is strictly prohibited.
- **Network Security:** Users are responsible for maintaining the security and confidentiality of their login credentials. Sharing accounts or passwords is prohibited. Users must not attempt to gain unauthorized access to any network resources, compromise the network infrastructure, or engage in any activities that may disrupt or interfere with the normal operation of the network.

- **Prohibited Content:** Users must not access, download, transmit, or distribute any content that is illegal or in violation of Oberlin College policies.

Blogging and Social Networking

Users using blogging and social networking, whether on college or personal devices, must follow this policy. Usage of college systems is allowed if:

- Conduct is professional and responsible.
- Confidential data is protected.
- Job performance is not affected.
- Information that could harm the college is not shared.

It is important to note that community members assume all associated risks when engaging in blogging and/or social networking activities.

Instant Messaging

College systems permit the use of instant messaging if it aligns with the college's policies and guidelines regarding the sharing of confidential data and does not have a detrimental effect on the job performance of employees.

Copyright Infringement

The use of the college's computer systems and network(s) for downloading, uploading, or handling illegal and/or unauthorized copyrighted content is strictly prohibited. Engaging in any of the above mentioned activities without permission from the copyright owner is considered a violation of the Acceptable Use Policy.

Privacy

While the College generally desires to maintain user privacy and to avoid the unnecessary interruption of user activities, the College reserves the right to conduct investigations as appropriate.

Personal Usage

Personal usage of computer systems is permitted if such usage follows the guidelines outlined in this document (and other policies) and does not have a detrimental effect on the college or the staff or faculty job performance.

Circumvention of Security Controls

Using any computer system or other mechanisms to circumvent the security controls or authentication mechanisms in place, access an end user's system, escalate access privileges or more, is strictly forbidden.

Software Installation

The installation of software on college computers is exclusively managed by CIT to safeguard against security risks like malware or spyware and ensure optimal system performance. Any software installation outside this protocol is strictly prohibited.

Access and Return of Assets Upon Termination

Upon termination of employment or contract, staff or faculty members must promptly return all Oberlin assets, regardless of their form, to the Center of Information Technology (CIT). The individual's work email will be directed to their supervisor or designated successor to ensure business continuity. This forwarded content will be accessible for a transitional period of three months, after which it will be permanently deleted. This process ensures the seamless transition of responsibilities while maintaining data privacy and compliance with our data retention policies. Any exceptions to this policy must be in writing and approved by CIT.

Remote Work and Off-site Security

Users must adhere to strict security protocols when engaging in remote work or taking college assets off-site. This includes using secure VPNs, end-to-end encryption, and robust authentication for remote access, ensuring physical security of devices, and adhering to data handling guidelines on personal or public networks. Additionally,

employees are responsible for the security of any equipment, information, or assets taken off-site and must promptly report any loss, theft, or security incidents to the Center of Information Technology, ensuring the protection of the colleges data and systems under all circumstances.

Equipment Provision and Peripheral Requests

Each employee is provided with one Windows or MacOS device, one monitor, and one keyboard and mouse. Should additional peripherals be required for job-related tasks, users must submit a peripheral request in the Services Portal to be approved by the requester's supervisor.

Personal Device Usage and Security

The use of personal devices for college activities is permitted under strict compliance with security and confidentiality protocols. Users must ensure their devices are secured with up-to-date antivirus software, firewalls, and robust authentication methods. Personal devices must only access college data through secure, approved methods, and any storage of sensitive information requires encryption. Unauthorized data transmission, storage, or processing on personal devices is prohibited. Compliance will be monitored, and breaches may result in disciplinary action, reinforcing the commitment to protect college data integrity.

Prohibited Activities

Users are prohibited from the following:

- Engaging in any activity that is illegal under local, state, federal or international law while utilizing Oberlin-owned resources or assets.
- Intentionally interfering with or denying service to another user.
- Introducing malicious programs into the Oberlin network.
- Intercept, attempt to intercept, or assist another in intercepting information not intended for that user's access.
- Circumvent, attempt to circumvent, or assist another in circumventing security measures protecting Technology Resources.
- Harassment of any form or violating the rights of any person or college.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type using Oberlin resources.
- The use of Oberlin College's electronic and computing resources for cryptocurrency mining activities or any form of cryptocurrency transactions
- Probe Oberlin College systems for vulnerabilities.
- Store or access Oberlin College Non-Public Information on a personally owned Desktop, Laptop, Mobile, or Other Endpoint Device.
- Forwarding/redirecting emails pertaining to work affairs to personal email accounts
- Knowingly causes physical damage to or attempt to repair a college-owned Desktop, Laptop, Mobile, or Other Endpoint Device unless they have written authorization to repair.
- Disclose or transmit confidential information regardless of whether they are authorized to access it.
- Use Oberlin College data outside of its intended purpose.
- Use Oberlin College environments or enterprise systems for experimentation or research purposes absent explicit authorization to do so.
- Use Technology Resources for commercial purposes not authorized by Oberlin College.
- Use Technology Resources for personal economic gain.
- Use Technology Resources for illegal or criminal purposes.
- Use of the internet to access inappropriate sites or forward information containing questionable or inappropriate materials.

Enforcement and Consequences

In the event of a violation of the Acceptable Use Policy, the college reserves the right to enforce disciplinary measures. These measures may include temporary suspension of network access, formal reprimand, mandatory

compliance training, termination of access privileges, termination of employment, student conduct processes, or legal action against the user.

Policy Review and Updates

This policy will be reviewed annually or as needed to adapt to new security threats, technological advances, or regulatory changes. This policy is subject to change at Oberlin's discretion, and CIT is responsible for maintaining the policy's relevance and effectiveness.

- **Last Revision Date: 06/10/2025**

Contact

For more information or inquiries about this policy, please contact CIT: **Services.oberlin.edu**, Website: **Oberlin.edu/cit**, Phone: **440-775-8197.**