OBERLIN
COLLEGE & CONSERVATORY

Policy #: 01.010

Policy Title: Acceptable Use Policy

Responsible Position for Policy: Chief Information Technology Officer

Office/Department Responsible for Policy: Center for Information Technology

Division Responsible for Policy: Finance and Administration

Scope: Individuals who directly, or through any agent acting on their behalf, interacts with Oberlin College Technology Resources, regardless of affiliation or location.

Original Issue Date: 01/11/2011

Last Revision Date: 05/04/2022

Log of Previous Revisions: 01/11/2011, 05/06/2015, 05/04/2022

Policy Purpose

The purpose of this Acceptable Use Policy (Policy) is to ensure that use of Oberlin College's Technology Resources respects applicable laws; Oberlin College policies, procedures, and codes of conduct; relevant licensing and contractual commitments of the College; and the rights of Oberlin College and its community members.

This Policy may be revised at any time to reflect changes in Oberlin's obligations and commitments and to reflect current technological state. This Policy is intended to serve as a guide to acceptable and unacceptable use of Technology Resources and should not be considered comprehensive. Users are encouraged to consult with the Center for Information Technology (CIT) on acceptable use issues not specifically addressed in this Policy.

Policy Statement

This Policy applies to individuals who directly, or through any agent acting on their behalf, interacts with Oberlin College Technology Resources, regardless of affiliation or location. All individuals to whom this Policy applies are responsible for becoming familiar with and following this Policy. While the Center for Information Technology is responsible for monitoring the use of Technology Resources, it is the responsibility of all individuals in the Oberlin College community to use Technology Resources in ways that support equitable access for everyone.

Users of Oberlin College Technology Resources *must:*

- Use only authorized Technology Resources and only in the manner and to the extent authorized by Oberlin College. Users and their supervisor are responsible for notifying CIT

when a change in their role necessitates an addition, subtraction, or modification of the Technology Resources to which they have access.
- Protect the security of accounts issued by Oberlin College. Users are responsible for any activity carried out under their Oberlin College accounts.
- Protect the security of Desktops, Laptops, Mobile, or Other Endpoint Devices issued by Oberlin College. Users are responsible for actions taken using their College-issued technology devices.
- Report the damage, loss, or theft of any Desktop, Laptop, Mobile, or Other Endpoint Device containing Oberlin College Non-Public Information to citpolicy@oberlin.edu;
- Report any breach, suspected breach, or discovered vulnerability of any Desktop, Laptop, Mobile, or Other Endpoint Device containing Oberlin College Non-Public Information to citpolicy@oberlin.edu; and
- Report any suspected violations of this Policy to citpolicy@oberlin.edu.

Users of Oberlin College Technology Resources *must not:*

- Intercept, attempt to intercept, or assist another in intercepting information not intended for that user's access, for example, by web scraping, network sniffing, or wiretapping;
- Circumvent, attempt to circumvent, or assist another in circumventing security measures protecting Technology Resources;
- 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;
- Knowingly cause physical damage to nor 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 and when the environment is designated for experimentation or research purposes;
- Use Technology Resources for commercial purposes not authorized by Oberlin College;
- Use Technology Resources for personal economic gain; or
- Use Technology Resources for illegal or criminal purposes.

Oberlin College reserves the right to take action, including the suspension of use privileges, where required by law, in case of potential College policy violations, and in any other case in which they deem it necessary or advisable for network integrity, security, and operations. 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.

Subject to the College's written agreement indicating otherwise, all individuals must return all Technology Resources when their employment or engagement with the College ends.

Scope

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

Definitions

Breach: Any incident that results in unauthorized access to data, applications, networks or devices.

Desktop, Laptop, Mobile, or Other Endpoint Device: Devices intended to be used directly by individuals and include, but are not limited to, desktops, laptops, mobile phones, and tablets.

Oberlin College Non-Public Information: Common examples of non-public information include FERPA, HIPAA, personally-identifiable data, non-public communications, student information, faculty and staff information, financial or financial transaction data. This definition reflects examples of Non-Public Information and is not intended to be exhaustive.

Environment or enterprise system: A collection of software, hardware, and networks managed by or operated on behalf of Oberlin College.

Sniffing: The practice of using software or hardware to monitor network traffic.

Technology Resources: Oberlin College-owned facilities, technologies, and information resources used for processing, transferring, storing, and communicating information. Common examples include enterprise environments, enterprise systems, computer labs, classroom technologies, computing and electronic devices, software and services, email, networks, telephones, mobile phones. This includes elements that are Oberlin College-owned, leased, operated, or provided by Oberlin College such as cloud and Software-as-a-Service (SaaS). This definition reflects examples of Technology Resources and is not intended to be exhaustive.

Web Scraping: The practice of extracting data from websites, either manually or by using a bot or web crawler.

Wiretapping: The practice of monitoring telephone and Internet-based conversations by a third party, often by covert means.

Administration

The Chief Information Technology Officer is assigned to administer this policy. This individual is responsible for keeping the policy up to date and coordinating a detailed review at least once every 5 years.

Related Information

This Policy is supported by additional policies that address specific technology uses and user groups. All CIT policies are available at https://www.oberlin.edu/cit/policies

Users should pay particular attention to the Protection of Personally Identifiable Identification Policy and Procedures (expected Summer 2022), governing the use of confidential data.