OBERLIN
COLLEGE & CONSERVATORY

Oberlin College & Conservatory

Title: Acceptable Use Policy (2021-2022)
Responsible Position for Policy: Center for Information Technology (CIT) Director
Office/Department Responsible for Policy: Center for Information Technology
Last Revision Date: 6/19/2020

Oberlin College provides a wide range of computing resources to support the educational mission and administration of the college. The Irvin E. Houck Center for Information Technology (CIT) provides and maintains the Help Desk, campus network, administrative systems, web servers and other servers, general and departmental computer labs and facilities, and institutionally owned desktop and laptop computers. CIT also provides audiovisual and educational technology support and resources.

The facilities of CIT are an essential resource for academic, administrative, and research processes for members of the college community. As such, all members of the college community are encouraged to use these resources, provided they respect the rights of others, abide by the rules and regulations of the college, and assume shared responsibility for safeguarding the college's computing environment. Proper and fair use is essential if all are to derive maximum benefit from them.

This policy may be modified at any time. Use of CIT resources is considered an agreement to abide by this policy. Users found in violation may be subject to penalties of varying degree, including temporary or permanent denial of access to CIT resources and services. Violators may also be subject to action by college, civil, or criminal judicial systems.

Guiding Principles

In making information technology resources available to all members of the college community, Oberlin College affirms its commitment to a free and open educational environment, conducive to learning and governed by legal and ethical principles. Oberlin College values the free flow of information. The college respects individual privacy, civility, and intellectual property rights. Because an electronic environment is easily disrupted and electronic information is readily copied, users of the college's resources are honor-bound to promote and protect these institutional values.

Under normal circumstances, college officials will not examine personal information transmitted over the network or stored on college-owned computers. However, the college reserves the right to monitor system resources, including activity and accounts, with or without notice, when:

1. It is necessary to protect the integrity, security, or functionality of college computing resources.
2. An account or system is engaged in unusual or excessive activity.
3. It has good cause to believe that regulations, rules, or laws are being violated.
4. In the event of health, safety, or security emergencies, as determined by authorized college officials.
5. When, due to the extended absence of an employee, demise of an employee, or termination of an employee for cause, as verified by the Chief Human Resources Officer or other authorized college official, it is necessary to retrieve vital college-related material.
6. Additionally, the normal operation and maintenance of the college's computing resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities as may be necessary in order to provide desired services.

Accordingly, all Oberlin College personnel are strongly urged to use college-provided resources **only** for college-related material and to acquire and use personal accounts and devices for any non-work-related material.

Note that any access made to an individual's account or data will be no more extensive than necessary. The account holder/data owner will generally be notified of access, either prior to or after access has occurred, when such notification will not be deleterious to pending or potential legal or security considerations.

User Responsibilities

Access to computing resources and network capacity is a privilege to which all college faculty, staff, and students are entitled. (Access may be granted to other individuals affiliated with the college or college personnel, as situations warrant and with approval from the director of information technology.) Certain responsibilities correspond with that privilege, including those listed below. Since no list can cover all possible circumstances, the spirit of this policy must be respected, namely; any action that hinders legitimate computer usage or invades the privacy of another person or institution is unacceptable.

1. **Use of CIT Facilities**
    a. All facilities of the Center for Information Technology, including those located in remote sites, are for the use of Oberlin College students, faculty, and staff. Spouses, partners, and children of members of these groups, with qualified needs, may apply to the Chief Information Technology Officer for the privilege of using CIT facilities. Residents of Oberlin, Lorain County, or others who have been granted library privileges are not automatically permitted to use CIT facilities.
    b. Users must not abuse equipment and are asked to report any mistreatment or vandalism of computing or network facilities to CIT staff (Mudd Level A) or to Campus Safety at (440) 775-8444. Food is discouraged in all CIT computer facilities, including remote sites operated by the CIT, because of potential harm to equipment. Beverages in approved containers (sturdy, covered, reusable containers) are allowed.
    c. Users should relinquish the computer they are using if they are doing nonessential work when others are waiting for a computer to perform course-related activities. Equipment should not be monopolized. Users should not use more than one computer at a time and should plan work so that the computer session is no longer than absolutely necessary. Game playing in CIT-maintained computer facilities/labs is prohibited at all times.
    d. Users should not install software, alter system files, or disconnect any cables on computers or other equipment.
    e. Users are expected to respect other users and the staff of the Center for Information Technology. Verbal or physical abuse of others, student or staff, will not be tolerated. A user must show an Oberlin College ID card to any CIT staff member or CIT student employee who so requests.
    f. Users must respect all notices (such as those concerning hours of operation, printing, etc.) posted in CIT facilities.
    g. Computers assigned to faculty and staff for the duration of their employment at Oberlin College remain the property of Oberlin College and as such, should be treated with appropriate care. These computers may be upgraded, as warranted, and must be relinquished in order for any required maintenance to be performed. Note that termination of employment may result in the immediate inability to access one's assigned computer. Accordingly, users are encouraged to use personally-owned computers to store or process personal materials.
2. **Legal Usage**
    a. Information technology resources may not be used for illegal or harmful purposes, including:
        i. intentional harassment of others;

ii. intentional destruction or damage to equipment, software, or data;
iii. intentional disruption or unauthorized monitoring of electronic communications.

b. Software is normally distributed under three kinds of licenses: proprietary, public distribution, and shareware. Unless otherwise indicated, users should assume all software made available by CIT is proprietary and may not be legally copied.
c. CIT will not knowingly provide support for software that a user possesses in violation of its license agreement. Consultants and staff may ask for proof of ownership before helping users with their software.
d. CIT will not knowingly allow illegally acquired software to be used on Oberlin-owned computers. CIT will remove any suspect software loaded onto Oberlin College-owned computers or servers.
e. CIT will not knowingly allow use of its resources (computers, equipment, network, etc.) for the illegal copying of digital media or files. Note: U.S. Copyright Law protects copyright owners from the unauthorized reproduction, adaptation, or distribution of digital material, including the unauthorized use of copyrighted sound recordings (e.g., music files), video files, and interactive digital software (i.e., video games).

3. Ethical Usage

a. Users should not use information technology resources, including personally-owned computers connected to the college network, for non-college, unsanctioned, or commercial activity.
b. Users should make no attempt to alter the condition or status of any computing network component in any manner.
c. Users should make no attempt to alter software other than their own, or to copy software intended only for execution.
d. Users should not interfere with, interrupt, or obstruct the ability of others to use the network or other CIT resources.
e. Users should not attempt to connect to a host via the network without explicit permission of the owner.
f. Users should not provide, assist in, or gain unauthorized access to college computing or network resources.
g. Users should not attempt to circumvent or defeat computer or network security measures.
h. Users should not systematically collect and use any privately or publicly available college data or content, including users' personal directory and account information, through the use of data mining, robots, or similar gathering and extraction methods.

4. Security

a. The college uses various measures to ensure the security of its computing resources. Users should be aware that the college cannot guarantee such security and should apply appropriate safeguards for their accounts, such as guarding their passwords and changing passwords regularly (required for e-mail accounts), and logging out of computers when done.
b. Users should be aware that data stored and used within OCApps (online applications powered by Google) is inherently non-secure, and is also not backed up. Thus, users must not place any confidential, sensitive, or personal data within any of the OCApps, and should not use OCApps as a primary storage location for vital data (alternative storage media should also be used).
c. Systems administrators of other departmental and individual computer systems are responsible for the security of information stored on those systems and for keeping those systems free from unauthorized access.
d. The default protection setting on CIT servers defines all files as belonging exclusively to their owner. Unless the owner changes the protection level, no file may be read, executed, or modified by users other than the owner. The only exception to this understanding is

that designated members of the CIT staff may examine accounts or files of users to investigate security problems, possible abuse of the Oberlin College computing system, or violations of regulations.

5. **Account Usage**
    a. Account holders should use only their own personal accounts unless given permission by an authorized member of the faculty, administration, or professional staff to use one that is designated for a specific purpose or job. Account holders may not allow others to use their personal accounts. The person holding an account is responsible for its use, and all activity originating from that account, at all times.
    b. Account holders should choose strong passwords, protect their passwords and keep them confidential. Passwords should be changed frequently. Any problem resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password) may be treated as grounds for action against the account holder. Any attempt to determine the passwords of other users is strictly prohibited.
    c. Account holders should not abuse any electronic mail, bulletin board, or communications system, either local or remote, by sending rude, obscene, or harassing messages (including chain letters) or by using these systems for non-essential purposes during the times when the computers are in heavy demand. Account holders should identify themselves clearly and accurately in all electronic communications, i.e., no anonymous postings and no spoofing of addresses. Unofficial mass e-mailings (i.e., spam) are prohibited.
    d. Account holders should use only their own files, those that have been designated as public, or those that have been made available to them with the knowledge and consent of the owner.
    e. Individual Oberlin College accounts (@oberlin.edu mail accounts, web accounts, etc.) are created for the express use of the individual for whom the accounts are created, but remain the property of Oberlin College. Accounts may be viewed in circumstances such as those delineated in paragraph B. above. Faculty and staff accounts may also be accessed to recover work-related information in the event of the termination of employment, or the incapacitation or demise of the employee. Accordingly, faculty and staff account holders are strongly urged to use a non-Oberlin account for personal correspondence.

6. **Network Usage**
    The following are responsibilities that are particularly applicable to users of Oberlin's campus-wide network.
    a. Only computers that have been properly virus checked, updated, and authenticated through established procedures may be connected to the campus network, unless otherwise authorized and established by CIT. Users must not attempt to circumvent this process.
    b. The person recognized as the owner of that authenticated computer system is responsible for that computer's use, and all activity originating from that computer, at all times.
    c. Excessive or improper use of network resources that inhibits or interferes with use by others is prohibited and will be cause for action by CIT, which may include restricting, limiting, or disabling network access.
    d. Users who connect computers to the network that act as servers have the additional responsibility to respond to any use of their server that is found to be in violation of this Policy.
    e. In no case shall the following types of servers be connected to the network: DNS, DHCP, BOOTP, or any other server that manages network addresses.

f. Due to the serious negative impact on network availability created by misconfigured routers and Wireless Access Points (WAPs), all routers and WAPS, except those configured and used by CIT, or devices which function as routers or WAPs, are disallowed.

7. Enforcement

Violations of this policy will be adjudicated, as deemed appropriate, and may include the following:

a. Loss of computing privileges
b. Disconnection from the network
c. Oberlin College Student Conduct action
d. Prosecution under applicable civil or criminal laws

Because of the rapid changes in technology, it is impossible to enumerate all of the circumstances that would constitute a violation of this Acceptable Use Policy. Additional circumstances that violate the spirit of the policy may be subject to the above penalties. Computer users should view the Center for Information Technology website for any updates to these policies (new.oberlin.edu/office/cit/).

Additional pertinent information and details may also be found there.