

Rules and Regulations (cont.)

Questions about reserve policies should be directed to the reserve supervisor in each library.

Fines for overdue reserve materials are listed in the Fines and Penalties chart. Because of the need to ensure reasonable access to required reading, fines for violating reserve regulations are stiff, and improper retention or removal of material is regarded as a very serious offense. Failure to respond to overdue notices has the effect of depriving others of access to the materials and may be taken as an Honor Code violation and dealt with accordingly before the Honor Committee. Repeated failure to return reserve materials on time may be referred to the college Judicial System for additional penalties.

Reserve fines should be paid at the Main Library circulation desk upon receipt of the fine notice. Unpaid fines totaling \$150 or more result in the student's borrowing privileges being suspended. Fines remaining unpaid at the end of the semester will result in a student's enrollment being held the following semester.

C. Building Rules and Penalties

Violation of established building rules may be grounds for fines and/or referral to the college Judicial System. For example, smoking is forbidden in all of the libraries, and when on and approaching the entrance ramp to Mudd Center; and is only allowed in the designated smoking area south of the ramp. In order to protect the collections from pest infestations, the possession of food is forbidden in all of the libraries except in areas especially designated for those purposes. Beverages are allowed in approved containers only. Possession of sound recording equipment is prohibited in the Conservatory Library. Furniture, typewriters, computer equipment, components of audio and audiovisual playback equipment, and other library equipment are not to be moved from their established locations or altered in any way. Defacement of library furnishings or parts of the physical buildings themselves is forbidden. Moreover, unauthorized entry in the building roof areas and unauthorized presence in the libraries after regular hours are both subject to disciplinary action by the college Judicial System and/or arrest and prosecution by local authorities.

Patron safety is of particular concern to the library. The sounding of an alarm bell requires all library users immediately to leave the building in an orderly manner. Failure to comply with this, or failure to follow the instructions of library staff, college, or city safety personnel may result in immediate disciplinary action by the college Judicial System.

D. Theft and/or Mutilation Rules and Penalties

Nothing is more reprehensible in an academic library than the theft or willful destruction of library materials. Theft is not only a crime against the library as an institution, but as an antisocial act it strikes at the vulnerability of an

open community. A person who conceals library materials while still on library premises, who improperly removes or damages equipment, books, journals, newspapers, manuscripts, maps, documents, recordings, video or audio tapes, computer software, or who fails to respond to repeated requests for return of materials may be subject to arrest and prosecution for theft in the local courts. If such an offender is an Oberlin College student, the librarian also reserves the option of proceeding against such offender through the Honor Committee and/or college Judicial System, where the penalties may include suspension or dismissal, as well as restitution of any losses suffered. Such offenses will be taken very seriously.

V. Policy for the Acceptable Use of Information Technology Resources

A. Introduction

Oberlin College provides a wide range of computing resources in order to support the educational mission and administration of the college. The Irvin E. Houck Center for Information Technology (CIT) provides and maintains the campus network, administrative systems, web servers and other servers, general and departmental computer labs and facilities, and institutionally-owned desktop and laptop computers. CIT provides additional services, including operation of a main Help Desk and an after-hours Help Desk, as well as sales and service of computers, peripherals, and software through the Oberlin College Technology Store. CIT also provides audiovisual and educational technology resources and support.

The facilities of CIT have become 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 campus, civil, or criminal judicial systems.

B. 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

Rules and Regulations (cont.)

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.

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.

C. 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 Director of Information Technology 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 The Office of Safety and Security 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 identify him or herself fully (e.g., by showing 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 should be treated as such. These computers may be upgraded, as warranted, and must be relinquished in order for any required repairs to be performed. Note that termination of employment could 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:
 - (1) intentional harassment of others.
 - (2) intentional destruction or damage to equipment, software, or data.
 - (3) 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.

Rules and Regulations (cont.)

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 AND 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 noncollege, unsanctioned, 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 nonsecure and is also

not backed up. Thus, users must not place any confidential, sensitive or personal data within any of the available 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 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 nonessential purposes during 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. 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 e-mail accounts, web accounts, etc.) are created for the express use of the individual for whom

Rules and Regulations (cont.)

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 may wish to consider acquiring a non-Oberlin account for personal correspondence.

6. NETWORK USAGE

The following are responsibilities that are particularly applicable to 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 an 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 Judicial Board 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.

VI. Policy for Academic Records

A. Academic Dates and Deadlines

All students are expected to follow academic dates and deadlines found in the events calendar at www.oberlin.edu or in the academic calendar available at www.oberlin.edu/regist.

B. Course Registration

1. All students currently studying on campus or expecting to return from a personal or academic leave are required to register for courses for the upcoming semester during November and April registration periods.
2. All students are also expected to complete the housing registration process.
3. If a student does not register for courses during the appropriate registration period, she or he may be withdrawn.

C. Enrollment

All students are expected to confirm that they have returned to campus through the online enrollment process in PRESTO.

D. Holds

A hold on a student's record may occur due to:

1. Failure to return library materials; complete a required meeting with a class or academic dean; submit required health forms; declare a major on time; or complete the housing registration process,
2. Outstanding financial obligations,
3. An incomplete financial aid application, or
4. Pending judicial or honor code issues.

A hold on a student's record may impact registration, enrollment, the receipt of a diploma at commencement, or marching at commencement.

E. Reinstatement

Any student returning from academic or judicial action, medical leave, or withdrawal must apply for reinstatement with Oberlin College. Complete procedures and policies are available at www.oberlin.edu/regist.

F. Transcripts

Official transcripts are available from the Office of the Registrar for \$6. Any request which requires expedited handling requires payment of a rush fee of \$30 (which includes the transcript and Fed Ex fee).