Computing Ethics and Responsibilities

Williams College provides computing and networking resources to students, faculty, and staff for a wide variety of purposes. These resources, networked for the general benefit of the community, are continually updated and maintained to provide an academic environment that is consistent with the educational goals of the College. These resources are limited, and how each individual uses them may affect the work of other members of the community and beyond, as our campus network is connected (through the Internet) to other networks worldwide. It is important that everyone be aware of their individual obligations and what constitutes proper use and behavior.

Williams College Computing Ethics and Responsibilities are available in the Student Handbook, the Administrative Handbook, and other publications of the College, as well as the Williams web site. Because of the rapid evolution of computing and information networks, the College reserves the right to modify these policies, with approval of the campus-wide Information Technology Committee, and publish the latest version on the OIT web pages. While users will be kept apprised of any changes, it is the user's responsibility to remain aware of current policies.

Common sense is a good guide to what constitutes appropriate behavior and use of computers and networks. You should respect the privacy of others and use computing resources in a manner that is consistent with the educational objectives of the College.

Behaviors that can create problems in a networked computing environment fall into the categories below. This list of responsibilities, while not exhaustive, should provide users with a good idea of what constitutes illegal or unethical on-line behavior. Users should note that computer users are governed by federal and state laws, including copyright laws, and College policies and standards of conduct. Report information security incidents or suspicious activity to OIT immediately.

Violations of these rules or, indeed, any disruptive situation in which a person's behavior or behavior generated on machines, accounts, or file space under that individual's control, creates a disruption of service to our clients, may be met by suspending access and services to the responsible parties. Access and services may only be restored following a discussion with the Office for Information Technology (OIT) and, if appropriate, other officers of the College.

The Office for Information Technology will not judge whether any request from a law enforcement agency to investigate suspected illegal activities affords due process and is of appropriate jurisdiction; OIT defers such requests to the appropriate officers of the College, and provides information required by subpoenas from courts with proper jurisdiction.

Malicious Activity

You may not attempt to gain access to computer systems (on or off campus) for which you have not been explicitly granted access.

You may not deliberately attempt to disrupt the performance of a computer system or a network, on or off campus. You may not attempt to 'break' system security. You may not reconfigure computer systems to make them unusable for others. You may not attempt to destroy or alter data or programs belonging to other users. You may not modify residential computing network services or wiring or extend those beyond the area of their intended use. This applies to all network wiring, hardware, and cluster and in-room jacks. Gateways and firewalls designed for home use, such as Cable/DSL routers and wireless access points, can disrupt the normal operation of the Williams network and are not allowed. You are responsible for protecting your computer and not allowing others to use your computer to attack others on the network. Specifically this means that you are required to be running a *supported*, up-to-date, anti-virus package and to ensure that your computer has had all applicable security patches installed.

You may not copy or redistribute software or other information that is copyrighted. By US law, software piracy is a felony. You may not attempt to override copy protection on commercial software. The ability to find and read information on computer systems does not mean that the information is in the public domain. Having the ability to read does not necessarily grant the right to copy or redistribute. Nor, even, in the case of certain information on the Internet, does ability to read mean that permission to read has been lawfully granted. Certain information is licensed to be read by the Williams community, though this does not grant the right to redistribute this information.

Privacy

All information on a computer system belongs to someone; some of it may be private or personal information; some may consist of confidential information, trade secrets, or classified material. If you have not been given direct permission to read or access another person's file, you may not try to do so. The

Williams network is a computing system covered by this policy. The operation of packet capture or port scanning software, or other means of snooping on another's network activity, is strictly forbidden.

Williams-specific or commercially obtained network resources may not be retransmitted outside of the College community. Examples include copyrighted course materials, electronic journals, other commercial information services from the Williams College Library, and private student and/or employee-related information such as home phone numbers, or addresses.

Williams College strives to ensure information privacy for its computer users. Occasionally legitimate reasons arise that require access to information held on college systems. These exceptions may be required based on legal action (such as a court order), may involve the health and/or safety of an individual or group, or be prompted by urgent college business needs and are covered by our emergency access procedures.

Forging, Password Sharing, Password Stealing

You may not attempt to impersonate another individual by sending forged information such as e-mail. You may not seek to determine another person's password, through cracking, decryption, interception or other means.

You must never give your password to anyone or use another person's password. Sharing passwords endangers you and makes our systems more vulnerable. Violations will be reported to the person's supervisor or department chair. OIT will never ask for your password under any circumstances.

No Solicitation or Harassment

Williams College has written standards of conduct that seek to prohibit annoyance and harassment by any members of the Williams College community.

You may not use computing resources to violate the College's standards of conduct. You may not distribute electronic chain letters, spam, or solicit for charitable or commercial purposes.

Negligence and Misuse (including private business)

Having access to computing privileges (e-mail account, Williams network connection, login, or shared file space owned by you), means that you have general responsibility for all computing activity which takes place from those accounts, connections, or file spaces. The College's connection to the Internet, for example, does not allow you to abuse that connection.

Access to the Williams College computing network and the Internet is limited to members of the Williams College community. Individuals within the Williams community are not permitted to provide access to the campus network to those outside this community. This restriction includes the operation of server software to provide any service that is accessible by those outside the Williams network without permission from OIT.

Use of Williams' Computing facilities is intended to be consistent with the educational mission of the College; this does not preclude personal uses. However, we note that the College has:

- for students: "Regulations covering student businesses" in the Student Handbook
- for faculty: "Other employment during the academic year" in the Faculty Handbook
- for administrative staff: "Employment outside Williams or beyond full-time with the College" in the Administrative Staff handbook

All place some limitations on the community's use of computing facilities for commercial purposes.

You should report any suspected illegal or unethical activity to the Office for Information Technology or the Dean's Office.

Copyright and Attribution Reminders

Misusing copyrighted material without the permission of the copyright holder is prohibited. Such acts are also a violation of the laws of the United States. Violators of copyright law could be subject to charges in state or federal court, and may also be sued by the copyright holder in civil court. To learn more about copyright, visit the Library's web page about copyright.

Illegal file-sharing using peer-to-peer file sharing programs is strictly prohibited both by College policy and under the Digital Millennium Copyright Act of 1998 ("DMCA"). The DMCA limits the liability of internet service and network providers (ISPs), including the College in its role as an ISP, in disputes between copyright holders and users of those services. The DMCA also establishes procedures through which copyright holders can obtain information from internet service and network providers about alleged infringing use of those services. These procedures make individual students, faculty and staff responsible for their illegal file sharing. and they must assume all resulting liabilities as individuals without support from the College. To learn more about how the College handles DMCA notices from the entertainment, music and other copyright holders, go to our policy about File Sharing and Copyright Violations.

Confidential Information

Williams College has both an ethical and legal responsibility for protecting confidential information in accordance with its Data Classification and Usage Policy. To that end, all classified data must be handled according to the policy.

In particular, all protected information must be stored and transmitted using only approved methods. Transmission of protected information by insecure messaging technologies (for example, email, instant messaging, SMS, chat, etc.) is prohibited, as is storage of protected information on mobile devices (laptops, phones, tablets, USB drives).

Print this page

« Copyright Infringement and File Sharing

Emergency Access of Information »

Covid-19 Information

Covid-19 is an ongoing concern in our region, including on campus. Safety measures are in place, and campus community members and guests are additionally advised to take personal precautions. See the college's Covid-19 website for information about campus policies. For the latest research and recommendations from the CDC, visit cdc.gov/coronavirus.

GET HELP!

Change Password	Password Changer
Guest Wireless	Williams Guest
Students	stchelp@williams.edu 413-597-3088
Faculty & Staff	itsupport@williams.edu 413-597-4090

Classroom Technology	413-597-2112
Report SPAM/Phish	Forward the email to **spam@williams.edu**
GLOW	FAQs
LinkedIn Learning	How to Sign-In
Cloud Services Status	Google, Glow, Panopto, etc.

SEARCH OIT

ANNOUNCEMENTS

JUL 13, 2022
A recent PayPal scam almost snagged a Williams community member

JUL 1, 2022
Google Data and Quotas for 2022

JUN 30, 2022
Collaboratively Optimizing Williams

View All →

OFFICE FOR INFORMATION TECHNOLOGY

Jesup Hall
22 Lab Campus Drive
Williamstown, MA 01267 USA
413.597.2094
413.597.4103
Norma.Miller@williams.edu

Back to top

Privacy Policy

Accessibility

Comment Form

Log In