# Reed College Computer User Agreement

*Approved by the Computing Policy Committee 9/16/2005. Revised: 11/21/2008; 2/3/2011; 3/10/11; 10/10/11; 10/2/2012; 10/15/2014; 11/19/2014; 3/15/2019; 12/12/2019; 3/5/2020; 3/6/2020; updated 11/15/2022; updated 11/13/2023*

Download the user agreement (PDF)

Reed College computing resources are provided for use by all Reed students, faculty and staff. Alumni and other individuals may use computer facilities by special permission, as guests of the College. All eligible individuals who wish to use the computing resources are required to read and accept this agreement and are expected to follow the guidelines for acceptable computer use described below.

## Acceptable Uses

The use of the computer facilities is granted to the undersigned only. The undersigned shall not allow another person to use their username and password. Reed's computing resources are provided primarily for academic purposes, including education, research, communication, and college administration.

## Prohibited Uses

It is prohibited to use Reed's computing resources in ways that:

- infringe on another individual's right to privacy or otherwise adversely affect members of the user community;
- are inconsistent with the academic mission and not-for-profit status of the College;
- violate usage restrictions required by Reed's software, hardware, ISP, or other technology or digital content licenses;
- violate College policies or local, state, or federal statutes;
- violate the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, privacy or similar laws or regulations. (for further information, see Reed's Copyright Policy)

Some examples of prohibited uses are:

- unauthorized use of another's account, identity, username, or password for reading, duplicating, deleting, or modifying electronic materials in the context of email, printing, faxing, copying, or by means of any other electronic resource provided by the College;

- unauthorized use or distribution of someone else's identity, username or password, to access remote computers via Reed's network facilities;
- intentional damage to hardware, software, network equipment, security devices, or other technology resources;
- intentional creation of malicious programs or introduction of such software into the Reed network (e.g., viruses, malware, worms, Trojan horses, e-mail bombs, etc.);
- attempting to bypass or destroy security measures specified by this and other Reed policies;
- the transmission of obscene, abusive, harassing, or threatening messages;
- non-academic use of network bandwidth or CPU cycles that adversely impacts resource performance;
- unauthorized use, duplication, or sharing of copyrighted materials, such as music, images, text, multimedia, commercial software, etc.;
- for-profit activities, such as development and sale of software or digital materials, or contract work unrelated to Reed's academic mission;
- not-for-profit activities unrelated to Reed's academic mission on behalf of an external organization unless previously approved in writing by the president of Reed College;
- use of Reed technology to obtain or transmit material that is in violation of sexual harassment, hostile workplace laws, or other state or federal laws;
- export of software, technical information, encryption software or technology, in violation of international or regional export control laws;
- providing information that is not publicly available about employees or students (including lists of such individuals) to parties outside of Reed College without authorization.

# Confidential Data

Reed College faculty, staff, and student employees have varying access to electronic information that is sensitive and confidential. Reed College considers the protection of such information and its electronic infrastructure from unauthorized use to be a key responsibility of all faculty, staff, and student employees. Failure to act in accordance with College guidelines may result in disciplinary and/or legal action.

Confidential information must be stewarded in an ethical, professional, and legal manner at all times. All institutional electronic data, regardless of how they are stored, remain the property of the College and are governed by this policy.

By law, certain institutional data may only be released with proper authorization, in compliance with applicable federal and state laws concerning storage, retention, use, release, and

destruction of data. Users are encouraged to seek guidance from an appropriate supervisor, senior officer, or the chief information officer if it is unclear whether or not specific information is confidential.

Confidential data shall be used only as required in the performance of College duties, and may not be inspected, copied, altered, deleted, shared, granted access to, or used in any other manner, except as required in the performance of those job duties.

Reed community members are responsible for the security, privacy, and control of data in their care, access privileges entrusted to them, and their username/password. If there is reason to believe that the user's username/password is known by or has been used by another person, the user must immediately notify an appropriate supervisor, senior officer, or the chief information officer. Reed community members must take every reasonable precaution to prevent unauthorized access to confidential data. Such data shall not be presented or shared inside or outside the College without prior approval from the appropriate supervisor or senior officer of the College. Confidential data should never be left on any device to which access is not controlled.

When using the institution's electronic information systems, care must be exercised to protect data from unauthorized use, disclosure, alteration, or destruction. Users must understand the definition of confidential information in the context of their job responsibilities and take steps to ensure that co-workers, staff, and student employees understand existing statutes and policies (such as FERPA, HIPAA, Donor Bill of Rights, Digital Millennium Copyright Act, GLBA, GDPR, etc., and College departmental guidelines that may supplement this agreement). Before granting access to confidential information, users should be satisfied that a "need to know" is clearly demonstrated. Users should seek guidance from an appropriate supervisor, senior officer, or the chief information officer when the appropriate use of, or the granting of access to, such information is unclear.

It is a violation of College policy, and may be a crime, for individuals to attempt to gain access to College electronic data that they do not need in the performance of their job or to which they are not authorized to have access.

**Use of Personal Devices or Services**

When handling restricted or highly sensitive college data, college employees are required to use ONLY Reed-provided technology resources. Such resources include Reed-owned equipment as well as Reed-managed online services and cloud services. Examples of restricted or highly sensitive college data, along with proper handling instructions, may be found in Reed's data classification and handling guidelines.

If you have questions or concerns regarding the appropriate way to handle specific data, please contact the Chief Information Officer (cio@reed.edu) for guidance.

**Use of Cloud Services**

Confidential or otherwise sensitive College information **must not be stored, shared, or otherwise processed** by a cloud computing service unless the service enters into a legally binding agreement with Reed, approved by the chief information officer, to protect and manage the data according to standards and procedures acceptable to the College.

Information Technology (IT) shall review requests for access to central data systems and serve as the initial point of resolution in instances where requests for such access conflict with this statement.

Appropriate College procedures shall be followed in reporting any breach of security or compromise of safeguards.

# Illegal Copying of Software and Other Copyrighted Materials

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of authors, artists, and publishers in all media including text, music, images, software and other domains. It encompasses respect for the right to acknowledgment and the right to determine the form, manner, and terms of publication and distribution of one's work. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical.

Copyright infringement and unauthorized access to digital materials may be grounds for legal action. Use of illegally copied software or other materials undermines Reed's ability to negotiate favorable software agreements and may result in legal action against the user as well as the College.

Reed prohibits the illegal use of copyrighted materials. Under the terms of the Digital Millennium Copyright Act (DMCA), the College is committed to respond to lawful requests for information. Reed will not protect or defend a user against criminal investigations or lawsuits resulting from intentional copyright infringement. (For further information, see Reed's Copyright Policy and the Reed Library Copyright & Fair Use webpage.)

# Fees

In general, the College does not charge students, faculty, or staff a fee for the use of computing or network resources. However, fees are charged in specific instances including:

- Printing: There is a per-page charge to students for printing to networked printers in the IRCs, Library, residence halls, and elsewhere. Students are billed through the Business Office. Information about current rates and charges can be obtained from Computer User Services or found on the web at: https://www.reed.edu/it/help/print/

- Stolen or damaged computers: Under certain circumstances, faculty and staff may be charged a fee in the event that College-provided computing equipment in their care is lost, stolen, or damaged beyond repair. A policy describing the details of potential employee liability are provided on the web at: https://www.reed.edu/it/policies/theft_loss.html

# Privacy, Storage and Transmission of Electronic Materials

The College respects each individual's right to privacy and takes steps to prevent unauthorized access to electronic materials stored or transmitted via College computing or network equipment. However, the College reserves the right to examine such materials at its sole discretion in certain cases; for example, when there is a potential violation of a law or of College policy.

Users should be aware that Reed's learning management system, Moodle, maintains logs of user activities. Faculty members and other Moodle site administrators have access to Moodle logs for their sites.

The College may use external service providers to store, transmit, or otherwise process user data. By endorsing this agreement, users agree that: (a) their data can be processed by external providers used by the College; and (b) they will abide by the terms of use and other policies of such providers insofar as those policies apply to Reed. A list of such providers is available from Information Technology.

Computer User Services is NOT responsible for personal files stored on hard drives in student Information Resource Centers (IRCs). Users are responsible for saving personal files to their own disk(s). IRC hard disks are erased on a regular basis and user-created files are deleted. Centralized disk storage is available to all students, faculty, and staff and may be requested by contacting Computer User Services.

# Email

The College uses email to communicate with members of the college community. Students, faculty, and staff are expected to check their email regularly.

Email is not a secure medium of communication. Users are reminded that the storage and transmission of electronic materials, including email, can be disrupted by hardware and software failure as well as by hacking. Users are cautioned about storing or transmitting material that is sensitive or confidential. It is the user's responsibility to back up their materials except for instances where the College specifically provides backup services.

# Mass Email

Mass emails are messages sent to large segments of the Reed Community, such as the entire faculty, staff, student body (or student class year), a curricular division, or a group of organizations. While such messages may seem like a good way to spread information to a wide audience, many recipients perceive them as spam or may even find them offensive. In order to avoid this problem, faculty, staff, students, or other members of the Reed community who wish to send a mass email need to follow these steps:

- first, determine the desired audience for your message (refer to the Reed Mass Email Lists described above);

- then, obtain approval to send an email to the desired email distribution list by following the Mass Email Guidelines
- then, email Public Affairs at mass-emails@reed.edu, indicating who has approved the message.

When Public Affairs confirms that you have received authorization to send your message they will provide guidance on technical details for sending the message.

Sending mass emails to the Reed community without authorization, by circumventing college distribution email lists or other means, is a violation of the Computer User Agreement and is subject to the penalties described in the *Failure to Comply* section below.

# Requests for Access to Email and other Files by Third Parties

From time to time, IT may receive internal or external requests for access to employee's or student's electronic mail and other files, including system, network, and user audit logs.

At no time shall IT staff members examine the contents of email or other user files in response to an access request by a third party unless so directed by the chief information officer, a senior officer of the college, or college legal counsel. In cases where a request is made as part of an eDiscovery process, IT response shall be governed by Reed College eDiscovery Guidelines.

Requests that do not fall under eDiscovery shall comply with the following guidelines:

- Requests for electronic materials must be made to the chief information officer and must specify the timeframe, the type(s) of electronic materials to be searched (emails, documents, etc.), well-defined search criteria (sender and/or recipient, header keywords, etc.) and the reason for the request;

- When a third party access request is made, the chief information officer shall consult with an appropriate senior officer and/or legal counsel to obtain written authorization prior to approving access;

- If access is approved, a IT staff member designated by the chief information officer shall contact the requester(s) to determine the optimal format for delivering the electronic materials and notify the chief information officer when the materials have been delivered.

# Failure to Comply

The College will suspend or revoke the computing privileges of anyone who violates this agreement or fails to pay a required fee. The terms and conditions of usage are subject to change as computing resources and user demands vary. This policy is reviewed on a regular basis by the Computing Policy Committee. The Reed community will be notified if the agreement is changed. The current version will be available on the IT website at: https://www.reed.edu/it/policies/user_agreement.html

Ongoing use of Reed's computing facilities and services implies a user's acceptance of the most current version of this agreement. Users who decline to accept the current version will be prohibited from using Reed's computing facilities and services.

If a computer user fails to comply with these terms and conditions, it will follow the "Procedures for Handling Violations of the User Agreement," located at: https://www.reed.edu/it/policies/violations_procedures.html

Other policies related to the use of Reed's computing resources may be found at: https://www.reed.edu/it/policies/

Access to the Internet via Reed's Internet Service Providers (ISP), must conform to both Zayo Group and Comcast Business Acceptable Use Policy available on the web at:

- https://www.zayo.com/wp-content/uploads/2015/09/Acceptable_Use_Policy.pdf
- https://business.comcast.com/customer-notifications/acceptable-use-policy

By accepting this agreement, the user acknowledges that he or she has read, understands, and agrees to comply with its provisions and other policies governing the use of Reed College computing and networking facilities. This agreement covers all computing equipment owned by the College as well as remote computing resources accessible through the College's communication facilities.

For further information, contact the Reed College Office of Computer User Services at 503-777-7525 or via electronic mail at cus@reed.edu

# Acceptance Declaration

I, _____, have read and understood the provisions and legal restrictions described above and other policies governing the use of Reed College computing resources referenced in this agreement. I understand that the agreement covers all computing resources owned by the College as well as remote computing resources accessible through the College's electronic communication facilities.

I further understand that use of Reed's computing resources is a privilege, not a right, and that if the terms of this agreement are violated the College may issue a warning, deny access to computing resources, refer for prosecution, or administer other penalties, depending upon the nature of the infraction.