Student IT Resources Acceptable Use Agreement

Introduction

Lower Columbia College (LCC) provides information technology resources to support faculty, staff, students, and members of the College community. These resources are available to support LCC's academic and administrative goals. The use of these resources to advance those goals takes priority. Internet service is provided by the **K-20 Education Network (k20wa.org/about/conditions-of-use-acceptance-policies/)** for educational purposes consistent with the educational mission of LCC. This Acceptable Use Agreement (AUA) is intended to protect the integrity and usability of these resources and to ensure their availability for both education and college business.

Scope

Users of LCC's IT resources agree to comply with applicable state, federal and local laws, Washington Administrative Code (WAC), including the **Code of Student Conduct (lowercolumbia.edu/publications/student-handbook/code-of-student-conduct)** , and **LCC policies and procedures (lowercolumbia.edu/publications/administrative-policies)** . The College's general policies apply to the use of IT resources just as they apply in all other College settings. This agreement supplements existing policies and procedures such as those that address ethical issues including academic dishonesty, copyright infringement, harassment, and plagiarism.

This agreement applies to students and guests who access or use LCC's IT resources. The access and use of LCC's IT resources provides acknowledgment and consent to follow all the rules and guidelines contained in this agreement.

Definitions

Hacked - A computer or device is considered hacked if it has been accessed or used without the owner's approval, or had its security features bypassed, or its operation otherwise compromised.

IT Resources - IT resources include but are not limited to computer hardware and software; electronic mobile devices; telecommunications, video and data networks; internet and cloud services; and electronically stored data. Use of these resources includes access from both on- and off-campus, as well as access from personal computers and electronic devices.

Pirating - The illegal copying or sharing of files or digital content that are protected by Copyright Law such as software programs, music, movies, games, etc.

Spamming - Inappropriately sending mass emails either to distribution lists or to individuals, or posting messages to multiple newsgroups.

Sexually Explicit Material - Sexually explicit material is defined in **RCW 9.68.130 (apps.leg.wa.gov/RCW/default.aspx?cite=9.68.130)** , but exempts authorized study and research in the areas of art, health, and science.

Prohibited Use of IT Resources

The College's IT resources are shared resources. Any activity that inhibits or interferes with the use of these resources by others is not permitted. Any use of these resources deemed inconsistent with the mission and purpose of the College is considered a violation of this agreement. Such activities include, but are not limited to, activities listed below.

1. Any use of College IT resources that engages or results in any of the following is prohibited:
   a. Discrimination or harassment based on sex, race, marital status, creed, age, national origin, sexual orientation, the presence of any sensory, mental, or physical disability, veteran status, or religious preference.
   b. Copyright infringement.
   c. Organized political or religious advocacy.
   d. Any unlawful activity.
   e. Disrupting or interfering with the experience of others who access or use the same resources.
2. College IT resources may not be used to send, receive, or display information including text, images, or voice that:
   a. Is sexually explicit, or that a reasonable person under the circumstances would consider obscene, abusive, offensive, or objectionable. "Sexually explicit material" is defined in **RCW 9.68.130 (apps.leg.wa.gov/RCW/default.aspx?cite=9.68.130)** , but exempts authorized study and research in the areas of art, health, and science.
   b. Harasses others with annoying, threatening, libelous or sexually, racially, or religiously offensive messages.
   c. Creates a hostile place to work or study.
   d. Consists of information which may injure someone else and/or lead to a lawsuit or criminal charges.
3. Users of College IT resources may not share network credentials with others, nor misrepresent their identity to gain access to College IT resources. Without

authorization, users may not access, modify, damage, destroy, copy, disclose, print, take possession of, or disrupt in any way the College's IT resources. This includes:

a. Gaining access by willfully exceeding the limits of authorization.
b. Gaining or attempting to gain unauthorized access through fraudulent means.
c. Gaining or attempting to gain access by using another person's name, password, access codes, or personal identification.
d. Gaining or attempting to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes.
e. Attempting to disrupt any resource from being available to other users.
f. Giving or publishing a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or email account, database, or any other College IT resource.
g. Loading or attempting to load any software on College computer systems.

Electronic Mail

The College email system is not a secure communications system. Users cannot expect privacy. By using the College email system, each user acknowledges:

1. The use of electronic mail is a privilege not a right. Transmitting certain types of communications is expressly forbidden. This includes messages containing chain letters, pyramid messages, and hoaxes; vulgar, obscene, or sexually explicit language or images; threatening or offensive content; derogatory, defamatory, sexual, or other harassment; and discriminatory communication of any kind. As with other IT resources, the use of email for commercial or political purposes is strictly prohibited.
2. All users of the College email system waive any right to privacy in email messages and consent to the access and disclosure of email messages by authorized College personnel. Accordingly, the College reserves the right to access and disclose the contents of email messages on a need-to-know basis. Users should recognize that under some circumstances, because of investigations, subpoenas, or lawsuits, the College might be required by law to disclose the contents of email communications.
3. Under the Electronic Communications Privacy Act, tampering with email, interfering with the delivery of email, and using email for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.
4. Inappropriate mass mailing, including multiple mailings to newsgroups, mailing lists, or individuals (also called "spamming") is prohibited. Users must honor others' requests to stop sending unwanted communications of any kind.
5. **Any user who suspects that his/her email account has been compromised is required to contact the IT Services department at (360) 442-2250 immediately**.

File Sharing and Copyright Infringement

Transferring copyrighted materials to or from any system, or via the College network, without the express consent of the owner of the copyrighted material is prohibited. Federal

copyright law applies to all forms of information, including electronic communications. Users should be aware that copyright infringement includes the unauthorized copying, displaying, and/or distributing of copyrighted material. All such works, including those available electronically, should be considered protected by copyright law unless specifically stated otherwise.

Illegal file sharing (also called “pirating”) falls under Copyright Law. Acts of piracy are violations of state and federal laws, and as such, may result in criminal charges. Illegal file sharing includes software programs, music, movies, games, and other digital files. Even if you are not aware that files you share are copyrighted, you may still be held legally responsible. There are legal alternatives to access copyrighted material. Educause maintains a list of legal options at **educause.edu/legalcontent (www.educause.edu/focus-areas-and-initiatives/policy-and-security/educause-policy/legal-sources-online)** .

Lower Columbia College complies with all provisions of the Digital Millennium Copyright Act (DMCA). Any use of the College network, email system, or website to transfer copyrighted material including, but not limited to, software, text, images, audio, and video is strictly prohibited.

Privacy

Users should not assume or expect any right of privacy with respect to the use of the College’s IT resources. Although LCC does not routinely monitor the communication of its employees or students, the College does monitor both data access and network use and maintains access logs, traffic reports and other data to ensure the stability, reliability, and security of its IT resources.

Authorized college employees may access or examine files or accounts that are suspected of unauthorized use or misuse, that have been corrupted or damaged, or that may threaten the integrity of the College’s IT resource. Files, email, access logs, and any other electronic records may be subject to search under court order.

Student Responsibilities

Students are responsible for all activities to and from their access accounts. Students must take reasonable precautions to protect access to their accounts, including using a secure password. Students must keep their passwords confidential and must not share passwords with anyone. Under no circumstances should a student allow someone else to share access to their account.

Students are responsible for taking reasonable precautions to secure and protect the integrity of their personal computers, mobile devices, and portable storage devices. In cases where a computer is "hacked," the student shall either shut down the system or remove it from the College network as soon as possible to minimize potential damage and to stop the attack from spreading.

Students are responsible for reporting misuse or suspected misuse of College IT resources, including unauthorized access to their personal equipment and accounts.

eLearning Student Expectations

1. **Keep Your Login Secure** - As an LCC student, you are responsible for maintaining the security of your usernames and passwords. Passwords may not be used by anyone other than the students to whom they are assigned. You are responsible for all uses of your accounts. Access to course materials is limited to only registered students. You are responsible for changing passwords periodically to maintain security.
2. **Originality of Coursework and Communication** - As an LCC student, you must complete your own online coursework and communication. Failure to do your own work may result in receiving a grade of "F" for the course. Any violation will be reported as an incident of academic dishonesty. For more information, see LCC's **Academic Dishonesty policy (lowercolumbia.edu/publications/student-handbook/academic-dishonesty)** located in the Student Handbook.
3. **Identity Verification** - As an LCC student, you are responsible for providing accurate and truthful information about yourself whenever identity verification is required.

Reporting Violations of the IT Resources Acceptable Use Agreement

Violations of this Acceptable Use Agreement should be reported immediately to the Vice President of Student Services at **(360) 442-2420** or to the IT Services department at **(360) 442-2250**. The College will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of this agreement will result in appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, or expulsion from the College, and legal action in accordance with Lower Columbia College's **Code of Student Conduct (lowercolumbia.edu/publications/student-handbook/code-of-student-conduct)** .