Employee Acceptable Use: Information Systems and Services

Administrative Procedure 701.1A

701.1A Information Systems and Services: Employee Acceptable Use

Lower Columbia College (LCC) employees and any other authorized users agree to comply with LCC's Acceptable Use Policy (AUP), including the following conditions:

1. Any use of College information systems or services that engages in or promotes any of the following is prohibited:
    a. Discrimination or harassment on the basis of 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. Personal political beliefs
    d. Personal religious beliefs
    e. Personal business interest, commercial uses, and solicitation on behalf of other persons unless approved by the President or a designee
    f. Any unlawful activity

2. It is the policy of Lower Columbia College to respect the copyright protections given by law to authors. It is against college policy for faculty, staff, or students to copy or reproduce any software protected by copyright or other means, or published information, except as expressly permitted in writing. College publishers must secure written permission to publish information, graphics, or photographs in which others may or could have a legally defensible interest.

    Copying, downloading, distributing, or sharing material, such as music, movies, games, software, or applications, for which the copyright holder has not specifically granted permission is against the law. Anyone installing software on college-owned systems is required to file proof of purchase and licensing information with the college's office of IT Services.

3. Lower Columbia College will maintain only one website, maintained by the Office of Effectiveness and College Relations.

4. With the exception of certain personal uses considered de minimis under RCW 42.52.160(3) and WAC 292-110-010, the College's information systems and services are provided exclusively for furtherance of college educational objectives, research, administrative processes, and College sponsored community service activities, and shall be used only for purposes consistent with the mission and goals of Lower Columbia College. Personal use of email and the Internet are

specifically included in the de minimis exemption only when such use complies with governing law and college policy. Internet based entertainment applications (games, music, video, or other) are not appropriate uses of college systems.

Personal use of college systems is allowed if the following conditions are met:

a. There is little or no cost to the state;
b. Any use is brief;
c. Any use occurs infrequently
d. The use does not interfere with the performance of official duties;
e. The use does not compromise the security or integrity of state property, information systems, or software;
f. The use is not for the purpose of conducting an outside business, in furtherance of private employment, or to realize a private financial gain; and
g. The use is not for supporting, promoting the interest of, or soliciting for an outside organization or group.

5. College computing 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. Authorized study and academic research are permissible;
    b. Harasses others with annoying, threatening, libelous or sexually, racially or religiously offensive messages; or
    c. Consists of information which may injure someone else and/or lead to a lawsuit or criminal charges.

6. All College information systems and services are the exclusive property of the College. Use of the College's information systems and services is a privilege, not a right, and is provided only to college employees, contractors, or other authorized persons for uses consistent with the mission and goals of the college. The College retains the right to determine when, how, for what purpose, and by whom such information systems and services may be used, and retains the right to deny access or use of such systems and services. In addition:
    a. In publications on the College's information systems and services and elsewhere, employees may not use the College's logo or other College owned materials unless specifically authorized to do so by Administrative policy, the College President, or designee.
    b. All materials stored or published on the College's information systems or services may be monitored, reviewed and/or removed by the President or a designee to prevent misuse of the system; during investigations of alleged illegal or inappropriate activity; and when necessary to conduct college business.
    c. Employees shall follow the Lower Columbia College Brand and Style Guide for all publications.

7. College employees are responsible for protecting the confidentiality, integrity, availability, and security of college data and information.
    a. Email messages that are deleted or moved to the trash are subject to automatic deletion after 30 days without possibility of retrieval.
    b. Cloud or Internet Services – Employees should not use consumer or personal storage services (Box.net, DropBox, personal Google Drive, OneDrive, YouSendIt, etc.) to store or share LCC data. These services are intended for individual consumers and data security measures may be downgraded to promote ease-of-use.
    c. Google Workspace – LCC has two Google educational domains for storing and sharing data and information:
        i. lowercolumbia.edu - This domain is for use by faculty and staff. It is FERPA-compliant and should be used for storing and sharing any official college documents, materials, or resources.
        ii. my.lowercolumbia.edu - This domain is for use by students. It is not FERPA-compliant and any documents, materials, or resources stored or shared here are considered temporary and disposable.
    d. Confidential Information – College employees must not share confidential or Personally Identifiable Information (PII) related to employees or students with unauthorized persons. College employees must report all breaches of confidential information to the Director of Information Systems.

8. College employees must not share private student information in violation of the Family Educational Rights & Privacy Act (FERPA).

9. College employees must take reasonable precautions to keep laptops, mobile devices and portable storage devices secure to prevent the theft of data.

10. Email messages, electronic files, Internet activities, and other network activities may be deemed public records under Washington's Public Disclosure Act (RCW 42.17A.001) and could, therefore, be disclosed upon request.

11. College email distribution lists are to be used for college business only. Distribution lists are not to be used to deliver personal messages including items for sale, photographs, stories, jokes, or opinions.

12. College employees will be assigned accounts to access college resources, services and systems. College employees must use their assigned account. College employees must not:
    a. Share their account information with anyone,
    b. Let another person use their account,
    c. Attempt to use another account,
    d. Use an account that has not been assigned to them,
    e. Use assigned accounts, college resources, services, and systems to engage in any transaction that is in conflict with the proper discharge of the employee's official duties. These business transactions can include, but are not limited to, unwarranted benefits or

gains to themselves, those of a family/household member (defined in Policy 227), or another person who would present a conflict of interest pursuant to Policy 225, in the form of:

i. Financial resources
ii. Grades
iii. Credentials
iv. Any other record modification leading to an unwarranted gain

Employees must follow all applicable state, federal and local laws, WACs, college policies, procedures and ethical standards. If an employee is uncertain about the best way to handle a situation or if a conflict of interest presents itself, they must consult with their supervisor or Human Resources for guidance.

College employees must report any suspicious activity involving their account to the office of IT Services as soon as it is discovered.

13. Email messages are subject to public records requests. Employees should have no expectation of privacy regarding the use of email. Employees should not use college email to send or receive private messages. Employees should ensure that all email use is professional.

14. College employees are required to use passwords that meet the current, approved password requirements. College employees must keep their passwords confidential and must not share passwords with anyone. College employees are required to change passwords when appropriate or when it becomes necessary.

15. College managers and supervisors shall enforce the Acceptable Use Policy when made aware of infractions. Instances of misuse that cannot be resolved informally will be referred to the College's Human Resource Department.

Historic Review:

- UMCC Review: February 21, 2023
- Governance Review: March 3, 2023
- Campus Comment: March 7-21, 2023
- Approved: March 22, 2023