Linfield College

Acceptable Use Policy

Information Technology Services

Revised: 2/12/2018

Approved: 2/27/2018

Overview

Linfield College’s intentions for publishing an *Acceptable Use Policy* are not to impose restrictions that are contrary to the institution’s established culture of openness and trust, but to inform all users of their obligation to comply with all existing laws and institutional policies in their use of information technology resources and systems.

Some rules for appropriate use of the College’s information technology resources and systems derive from legal considerations. The College must address actions that may violate Federal compliance requirements (e.g., financial aid) as well as its agreements with outside vendors. Additionally, these rules are intended to ensure that College resources are used to advance the College’s mission.

Purpose of Policy

The purpose of this policy is to outline the acceptable use of Linfield College’s information technology resources and services. These rules are in place to protect the employees, students, and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. It is the responsibility of every user to know these guidelines, and to conduct their activities accordingly. This policy may be reviewed and amended annually or as the need arises.

Scope

The term "users," as used in this policy, refers to all employees, students, independent contractors, and other persons or entities accessing or using Linfield College’s information technology resources and services, wherever the users are located.

This policy applies to all information technology resources and services whether owned or leased by Linfield College, the employee, or a third party. Information technology resources and services include, but are not limited to, the following: host computers, file servers, workstations, standalone computers, laptops, tablets, smartphones, software, and internal or external communications networks (Internet, commercial online services, web sites, and e-mail systems).

The information technology systems belonging to Linfield College are to be used for College business and educational purposes in the course of normal operations.

Policy

General Use and Ownership:

Linfield College confidential information stored on electronic and computing devices whether owned or leased by Linfield College, the employee or a third party, remains the sole property of Linfield College. You have a responsibility to report within 24 hours the theft, loss or unauthorized disclosure of Linfield College equipment or confidential information to the department of Information Technology Services (ITS). You may access, use or share Linfield

College confidential information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use outside of the normal scope of work and in accordance with Linfield policies and standards. Incidental personal use is permissible to the extent that it does not violate other provisions of this policy, interfere with the performance of the employee's duties, or interfere with the education of students at the College. The use of social media by employees is also subject to the terms and restrictions set forth in this Policy.

For security and network maintenance purposes, authorized individuals within Linfield College may monitor equipment, systems and network traffic at any time. Users should not have an expectation of privacy in anything they create, send, or receive on their network-attached computers.

Unacceptable Use:

The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Linfield College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College owned or leased resources. The lists below are by no means exhaustive, but an attempt to provide a framework for activities that fall into the category of unacceptable use.

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Linfield College. This includes installing software licensed by the College on a personal device, unless the license specifically permits such use.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license is strictly prohibited. For exceptions to the copyright restriction, please see the Linfield Library Copyright Policy.
3. Accessing College data, a server, or an account for any purpose other than conducting business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others either deliberately or through failure to secure its access.
7. Using a computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification to Linfield College ITS is made and approved.
10. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal duties.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
13. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
14. Any form of harassment via email, telephone, or social media whether through language, frequency, or size of messages. Fraudulent, harassing, obscene, or other unlawful material may not be sent by e-mail or other form of electronic communication.
15. Unauthorized use, or forging, of email header information.
16. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
17. Using a College resource for the transmission, creation or storage of commercial activity, personal advertisements, solicitations, or promotions outside of the employee's normal scope of duties.
18. Providing confidential information about employees, donors or students to parties outside Linfield College.

Related Standards, Policies and Processes

Linfield Library Copyright Policy
Linfield Catnet Account Policy
Email as the Official Means of Communications Policy

Policy Compliance

Linfield College will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and community feedback to the policy owner.

All users must comply with the College’s policies. When a member of the College community is found to be in violation of this policy, the College’s disciplinary process will be followed as outlined in the personnel handbooks.   If the matter involves illegal action, law enforcement agencies may also become involved, as would occur for matters that do not involve information technologies or the Internet.

Use of Linfield College’s information technology resources and services constitutes acceptance of this *Acceptable Use Policy*.