Lakeland Community College

POLICY TITLE:	INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY
POLICY NO:	3354:2-11-03
ORIGINALLY APPROVED DATE:	01/15/98
REVISED DATE:	03/07/25; 09/29/22
EFFECTIVE DATE:	03/07/25
NEXT REVIEW DATE:	03/2030
RELATED PROCEDURE:	BT11-02A Electronic Communication Procedure ITS25-05 Computer & Communication Hardware/Software ITS25-XX Written Information Security Procedure
RESPONSIBLE OFFICE(S):	ADMINISTRATIVE TECHNOLOGIES
APPROVED BY:	BOARD OF TRUSTEES

A. Purpose and Scope
    1. The purpose of this policy is to outline the acceptable use of college-owned or leased technology resources, specifically providing guidelines to protect against the inappropriate use of such resources leading to an increased risk for virus attack, compromised network systems, and services and/or illegal activity.
    2. This policy applies to information and technology (including, but not limited to computer equipment, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), related hardware, operating systems, storage media, internal networks and network accounts, email, internet, and cloud service) that is owned or leased by the College and provided in furtherance of the College's mission and/or in support of its administrative and academic activities.
        a. Technology resources as defined above are to be used for serving the interests of the College, our students, and the community.
        b. College proprietary information stored on electronic and computing devices whether owned or leased by Lakeland, the employee or a third party, remains the sole property of Lakeland and will be secured through legal or technical means in accordance with relevant policies: Data Security and Privacy Assurance (3354:2-11-04), Identity Theft Protection (3354:2-11-05), and FERPA Policy for the Confidentiality and Review of Student Records (3354:2-63-01) and Written Information Security Procedure.

B. General Use and Ownership Access
    1. All employees, students, contractors, consultants, third-party vendors, service providers, and stakeholders of the College are responsible for exercising good

judgment with respect to the appropriate use of information and technology as defined above in accordance with the College's policies, procedures, and standards, as well as local, state, federal, and/or international laws and regulations.

2. Stakeholders may access, use, or share College proprietary information only to the extent it is authorized and necessary to fulfill assigned responsibilities of the stakeholder's role. Stakeholders have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the College's proprietary information.
3. Upon separation from employment or contract termination, all provided electronic equipment and associated data must be returned to the College. If the electronic equipment is not returned by the date of termination or separation, any remaining payroll owed to the individual will be withheld until the equipment is returned in good condition.
4. Individual departments are responsible for creating guidelines for the personal use of internet/intranet/extranet systems. In the absence of such guidelines, employees should refer to College policies including but not limited to the following minimum access standards for all mobile and computing devices connecting to the College's internal network:
    a. System level and user level passwords must comply with minimum password standards:
        i. A minimum number of 7 characters.
        ii. At least 2 alpha and 2 non-alpha characters.
        iii. Not be a part of username, not be a dictionary word, or contain more than 3 consecutive characters or numbers.
    b. Authentication and security standards:
        i. All mobile devices must have authentication enabled to gain access to the device.
        ii. All computing devices must be secured with a mobile security enabled authentication (finger scan/PIN/facial scan) or password-protected screensaver with the automatic activation feature set to 10 minutes or less, unless Administrative Technologies approves an exception.
        iii. Employees must lock the screen or log off when the device is unattended.
        iv. Security updates and patches shall be applied in a timely manner, or automatically when possible.
        v. The operating system must be supported by the developer.
        vi. Anti-virus shall be installed and updated automatically or in a timely manner, when possible.
        vii. Users must not leverage the "Remember Me" or "Remember my Password" function inside of a browser on a shared or public device.
        viii. Users must not connect enterprise assets to open, unencrypted WiFi networks.

ix. Users must be aware of their surroundings when working remotely to ensure others are not shoulder surfing or viewing sensitive material.

c. Miscellaneous:
   i. Files including personal data must be encrypted before being transferred electronically.
   ii. Providing access to another individual, either deliberately or through failure to secure its access is prohibited.
   iii. Postings by employees from a college email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Lakeland, unless posting is while performing business or educational responsibilities.
   iv. Employees must use extreme caution when opening emails that may appear to contain malware and contact Administrative Technologies for assistance.

5. When using enterprise resources, the user shall have no expectation of privacy. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by law.
6. The College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. For security and network maintenance purposes, authorized individuals within Administrative Technologies may monitor equipment, systems, and network traffic at any time.
7. Users leveraging their personal device to store enterprise data may have their device completely wiped. Reasons for device wipe may include: lost/stolen device, termination of user's employment, compromised/hacked account or device.

C. Unacceptable Use
1. Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College-owned resources. The non-exhaustive list of activities below is generally prohibited unless an employee is exempted from these restrictions while performing 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).
2. Prohibited Activities Related to System and Network Access
   a. Violating 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 software products that are not appropriately licensed for use by the College.

b. 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 College or the end user does not have an active license is strictly prohibited, unless following the rules for fair use for educational purposes.
c. Accessing the College data, servers, or accounts for any purpose other than conducting the College business, even if access is authorized.
d. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
e. Revealing account passwords to others or permitting others to use personal accounts (apart from Administrative Technologies employees working to setup or repair an issue).
f. Using a college computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
g. Making fraudulent offers of products, items, or services originating from any College account.
h. 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.
i. Port scanning or security scanning unless prior notification is made to Administrative Technologies.
j. 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 job/duty.
k. Circumventing user authentication or security of any host, network, or account.
l. Introducing honeypots, honeynets, or similar technology on the College network.
m. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session via any means, locally or via the internet/intranet/extranet.
o. Providing private non-directory information about college employees to parties outside Lakeland, unless legally required or as part of contracted college systems.

p. Enterprise data must not be stored on non-enterprise, personal cloud provider platforms (e.g., Google Drive, Microsoft OneDrive, Dropbox).

3. Prohibited Activities Related to Email and Internet Access
    a. Sending unsolicited external email messages, including the sending of 'junk mail' or other advertising in bulk to individuals who did not specifically request such material (email spam) unless an exception is coordinated through the Marketing Department, following their guidelines.
    b. Harassment via email, telephone, text, or paging whether through language, frequency, or size of messages.
    c. Unauthorized use, or forging, of email header information.
    d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
    e. Creating or forwarding 'chain letter', 'Ponzi', or other 'pyramid' schemes of any type.
    f. Using for private or personal business or for other for-profit activities or institutions.
    g. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).
4. Prohibited Activities Related to Social Media Use
    a. Limited and occasional use of the College's systems to access and engage in social media platforms for personal use is acceptable if it does not otherwise violate College policy and does not interfere with an employee's regular work duties. Social media use from the College's systems is also subject to monitoring.
    b. Policies noted in A(2)(b) above apply to social media. As such, employees are prohibited from revealing any College confidential or proprietary information, trade secrets, private personal data or any other material covered by Lakeland's policies when engaged in social media.
    c. When representing the College or running a college-based social media site, employees are prohibited from:
        i. Engaging in any social media that may harm or tarnish the image, reputation and/or goodwill of the College and/or any of its employees.
        ii. Making any discriminatory, disparaging, defaming, or harassing comments or otherwise engaging in any conduct prohibited by the College's Non-Discrimination and Anti-Harassment policy.
        iii. Attributing personal statements, opinions, or beliefs to the College. Employees expressing their own beliefs and/or opinions in social media may not, expressly or implicitly, represent themselves as an employee or representative of the College, but may clearly indicate that the "opinions expressed are my own and not necessarily those of the College."

iv. Using the College's trademarks, logos, and any other College intellectual property in connection with social media activity without permission from the Marketing Department.

D. Policy Compliance

1. Users who are aware of any event which threatens the availability, integrity, or confidentiality of enterprise data, or which breaches any standard, policy, procedure, or any associated requirement, or is contrary to law, must immediately contact Administrative Technologies or their immediate manager.
2. Administrative Technologies will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.
3. Any exception to the policy must be made in writing and must contain: the reason for the request, the risk to the enterprise of not following the written policy, the specific mitigations that will not be implemented, the technical and other difficulties, and the date of review. Exceptions must be approved by Administrative Technologies in advance, with disputes reviewed by the Data Assurance and Privacy Assurance Committee.
4. Any person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or expulsion.
5. The Board directs the President, in collaboration with the Data Assurance and Privacy Assurance Committee, to review and update the Written Information Security Procedure on an annual basis.