Information Technology Policy

As a place of learning and teaching, Lakeland University thrives on an open exchange of information. Lakeland's computer information systems and networks make that exchange of information possible and are, therefore, an integral part of the university's business. Lakeland University encourages the use of its information technologies to support research, enhance instruction, and act as a resource for the needs of the campus community.

To provide these services and protect its information systems, Lakeland University requires that members of its educational community use these resources in a manner consistent with the goals of the university. Users of Lakeland University equipment, software, and computer accounts are expected to follow acceptable standards of ethics and conduct in their use of computing resources. All Lakeland University faculty, students, and staff should be aware of the following information technology security policy and its requirements and guidelines.

1. Every computer and computer account issued by Lakeland University remains the property of the university. Individual users, however, are responsible for their own accounts and the way those accounts are used for as long as they are members of the Lakeland University community. This means users can expect the contents of their accounts are private, safe, and secure; nonetheless, those users must help to maintain security by, for instance, keeping their password a secret, restricting use of their account, and using their accounts in an appropriate way. Using another person's account or allowing someone else to use an account makes both parties potentially liable to corrective action, up to and including termination. If you believe an account has been violated or misused, please contact Lakeland University's Information Technology department.
2. To adhere to FERPA regulations, use of mobile devices that connect to Lakeland University's Exchange server and any other Lakeland University data must be password protected. Users requesting access to email on mobile devices must adhere to this policy and accept the electronic security policy applied by the server. Mobile device passwords must be at minimum, a four-digit PIN. However, users could use a full complex password if they wish, as well.

   Lakeland University reserves the right to wipe all Lakeland University data from a device if:
   a. the device has had more than eight attempts to enter the password on the device
   b. the device is lost or stolen and has any access to Lakeland's data. Reporting to the Information Technology department is mandatory.
3. There are three types of accounts used to access Lakeland University Information Technology assets; Academic, Administrative and Alumni.
   a. Academic accounts are provided to students. Academic accounts are used to access Lakeland University academic resources.

b. Administrative accounts are provided to Lakeland University employees. Administrative accounts are used to perform Lakeland University business-related activities.
c. Upon request, Academic accounts may be converted to Alumni accounts after graduation. Alumni accounts are e-mail only accounts provided to Alumni of Lakeland University.
    i. If an email account has not been accessed or inactive in a six month period, the email account will be disabled.
    ii. After an additional six months with no activity, the account will be permanently deleted.
d. Under ***no circumstances*** will an Academic account be granted access to or be used for Lakeland University business activities.
e. No account used for Lakeland University business can become an Alumni account.

4. Some uses of Lakeland University's information technology are prohibited. Providing unauthorized access to Lakeland University network and/or resources to an outside user not related to the university is prohibited. Unauthorized uses include, but are not limited to:
    a. uses that violate the law, including the violation of copyright law;
    b. uses that have a significant negative impact on the safety and security of other members of the Lakeland University community, including the transmission of threatening or harassing materials;
    c. uses that threaten to disrupt network services or equipment, including the distribution of unsolicited advertising, unsolicited mass email, improper/excessive use of data storage space, or items designed to propagate computer viruses;
    d. uses that invade the privacy of others, including attempts to gain unauthorized entry to the contents of others' computers or accounts;
    e. uses that violate the property rights of Lakeland University, including attempts to profit financially from the University's information technology systems and/or access to those systems;
    f. uses that interfere with the expectations of Lakeland University as an employer, including excessive private or personal business.
5. Lakeland University respects and values the privacy of its students and employees, and the data contained within computer accounts issued by Lakeland University are private. Expectation of privacy does not survive a situation of termination. As noted above, unauthorized access to those accounts and to that data is prohibited.
    a. In some circumstances, however, Lakeland University must make exceptions to its users' expectations of privacy – to protect the system as a whole, to protect the privacy of other users, and to protect the name and interests of the university.
        i. If there is probable cause to believe that a computer account contains information relevant to a Lakeland University interest or legal proceeding – including evidence of the prohibited uses listed above – a person other than the authorized user may examine such data files or programs. Depending on the user involved, permission for such access is granted by the Lakeland University President, the Director of Human Resources, or

the employee's area Vice President. At least two of the above must approve any such access.

ii. Access to accounts and/or data by the Information Technology department for routine system maintenance or to create backup copies is permitted and does not violate users' expectations of privacy.

6. Misuse or tampering of Lakeland University's computing resources may result in one or more of the following punitive measures (which do not exclude criminal penalties for violations of state or federal law):
    a. loss of access to computer resources;
    b. required repayment of funds expended in unauthorized use;
    c. corrective action;
    d. suspension or expulsion from the University;
    e. termination of employment;
    f. legal action.
7. As information technology and the threats against it are continually changing, the Information Technology department will routinely provide additional information and instruction about the proper and productive use of the university's computer systems and networks which will be posted on the IT Help Desk tab on my.lakeland.edu.
    a. Whenever possible, account users should attend to this information and follow instructions provided.
    b. These informational updates will help Lakeland University to ensure the best possible system performance for all members of its educational community.
8. The Lakeland University Information Technology department provides wireless access to students, staff, faculty and guests of the university. Non-Lakeland owned access points can and will interfere with the service being provided by Lakeland University, thus impacting our overall customer service. Under no circumstances is anyone allowed to connect or operate a personal wireless access point on the Lakeland University campus.
    a. Residence Hall Directors or other university employees are expected to inform students of this policy and request students power down any access points they are running as they become aware of them.
    b. Staff and faculty are expected to report any non-Lakeland access points they become aware of to the Information Technology department via the Help Desk.
    c. If there are areas not covered by Lakeland access points, please inform the Information Technology department and we will make our best effort to increase coverage to that area.
9. Due to technological advances and evolutions, Lakeland University reserves the right to amend this policy in the future as deemed necessary and appropriate. Proposed changes will be discussed with members of the university community and will be reviewed and approved by the Executive Leadership Counsel prior to implementation.