Lander UNIVERSITY

Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

ACCEPTABLE USE POLICY

A. INTRODUCTION

This policy governs the use of computers and computer networks at Lander University. As a user of these resources, you are responsible for reading and understanding this document. Lander University encourages the use of the Internet to support the research, instruction, and public service missions of the institution. Thus, this policy is not meant to infringe upon the principles of academic freedom. However, the wide array of new resources, new services, and interconnectivity available via the Internet exposes the University to a variety of risks. In response to these risks, the University has adopted this as its official policy regarding Internet use. This policy supplements and should be read in conjunction with other University policies.

B. APPLICABILITY

This policy applies to all Faculty and Staff members who use the Internet with University computing or networking resources. All Internet users are expected to be familiar with and comply with this policy. Any questions regarding this policy should be directed to the Office of Information Technology Services at 388-8234. Violations of this policy can lead to revocation of system privileges and/or disciplinary action including termination.

C. USER ANONYMITY

Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or the University's information resources technology system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings.

D. PERSONAL USE

Although personal use of the Internet for nonbusiness activities, such as games and news groups, is allowed, Lander University recommends that the use of this resource be reserved primarily for academic purposes. Infrequent use of University computing resources for personal purposes is permissible so long as University business activity is not affected by this personal use.

E. APPROPRIATE BEHAVIOR

Although Lander University recognizes the principle of academic freedom, the University is bound by local, state, and federal laws regarding electronic media. Thus, to avoid libel, defamation of character, and other legal problems, whenever any affiliation with University is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, threats against another user or organization over the Internet are also prohibited. All Internet messages and materials intended to harass, annoy, or alarm another person are strictly prohibited. This includes messages and materials that are inconsistent with University policies concerning “Equal Employment Opportunity”; “Sexual Harassment and other Unlawful Harassment.” Any individual who violates this policy shall be subject to discipline, up to and including discharge. Conduct which violates this policy includes, but is not limited to, the following:

- Sending, storing, or accessing obscene messages and/or materials;
- Unauthorized attempts to view and/or use another person's account;
- Using computers, accounts, and/or networks to gain unauthorized access to University systems or other systems;
- Using University resources for commercial activity such as creating products or services for sale;
- Copying software protected by copyright, except as permitted by software licensing agreements; and
- Chain letters and broadcast charitable solicitations.

F. NO PRIVACY EXPECTATIONS

Faculty and Staff members using University information resources systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. As such, you should avoid sending information over the Internet that is considered to be confidential or private. In addition, Lander University expressly reserves the right to examine electronic mail messages, individual computer files and documents, web browser cache files, web browser bookmarks, and other information stored on or passing through University computers. University officials may conduct such examinations at any time and without prior notice to assure compliance with internal policies, assist with internal investigations, and assist with the management and protection of University information resources systems. Please note that in certain situations the University may be compelled to access and disclose information sent over its Internet and e-mail systems to law enforcement authorities.

G. INFORMATION SECURITY

As Faculty and Staff members with access to University information systems, you are responsible for ensuring that your use of these resources does not compromise the integrity or security of any University data or system. Any sensitive information, including student records, accessible to University employees must be protected in accordance with federal and state privacy laws, as outlined in the Information Privacy & Security Plan. All University employees are expected to practice behavior consistent with information security requirements, including but not limited to:

- Completing security awareness training as needed;
- Preventing unauthorized access to any University-issued computer or device;
- Locking the screen or signing out of any system if leaving it unattended;
- Protecting any passwords and login credentials by not sharing them or leaving them visible to the public;
- Maintaining strong, current passwords and using separate passwords for different systems; and
- Reporting immediately to ITS any suspicious email or computer activity, as this may be evidence of phishing or malware.

Failure to comply with this policy can result in loss of system access and/or other disciplinary action, up to and including discharge.