Hannibal-LaGrange University
COMPUTER USAGE POLICY

Origination Date: **5/17/96** **Technology Committee** **Approved by Administrative Cabinet** Revision Date: **06/4/24** Revision: **AC**

Introduction

Campus computing is intended to support the mission of Hannibal-LaGrange University in providing a relevant education anchored in a Biblical worldview and requires responsible, ethical and legal use of computer resources. All students, personnel and other users are expected to abide by the guidelines set forth in this policy. Access to campus computer resources is a privilege contingent on the following: availability of the resources, current academic priorities, adherence to this (and subsequent) computer usage policies, and payment of necessary fees.

The University extends the Computer Usage Policy principles and guidelines to systems outside HLGU accessed via HLGU facilities (e.g., electronic mail or remote logins using HLGU's Internet connections). Networks or computing providers outside the University may impose additional conditions of appropriate use, for which you are responsible.

This policy pertains to anyone who will be utilizing HLGU computer or network resources in any way. If someone has questions about policy guidelines, or allegations of harassment or other irresponsible use of technology resources, he or she should contact the Office of Computer Services (OCS). The Office of Computer Services is located on the first floor of the administration building and may be contacted by phone at 573-629-3032 or by email ithelpdesk@hlg.edu.

Definitions

Users are people who have been assigned a network account such as employees or students.
Third-party vendors are vendors with which HLGU has contracted services, software or equipment.
Guests are visitors to the HLGU campus. Guests are subject to the same responsibilities and conditions as users but will not have the same privileges. Guests are only allowed access to the Public Wi-Fi.

I. User Responsibilities

University computing resources are available for the purpose of advancing the University’s mission. Faculty, staff, and students may use them for purposes related to their studies, their responsibilities for providing instruction, the discharge of their duties as employees, their official business with the University, and other University-sanctioned or authorized activities. The use of University computing resources for commercial purposes including any sort of solicitation is prohibited.

The University acknowledges that occasionally individuals use University computing resources assigned to them or to which they are granted access for non-commercial, personal use. Such occasional non-commercial uses are permitted by faculty, staff, and students, if they are not excessive, do not interfere with the performance of any faculty, staff member, or student’s duties, do not interfere with the efficient operation of the University or its computing resources, do not disrupt classroom activities and are not otherwise prohibited by this policy or any other University policy or directive. Decisions as to whether a particular use of computing resources conforms to this policy shall be made by the Director of Computer Services or appropriate administrator.

Acceptable behavior includes, but is not limited to the following:

1. Using resources for University courses, research, functions, and appropriate correspondence.
2. Respecting copyright and other intellectual property rights. (See Additional Matters Section: D, E, & G)
3. Abiding by security restrictions on all systems to which the user has access.
4. Using personal account(s) properly (i.e. changing passphrases as recommended by the Office of Computer Services and not sharing them.)

Unacceptable behavior includes, but is not limited to the following:

1. Cheating, plagiarism, information theft or academic dishonesty including purchasing papers off of the Internet.
2. Wasting limited resources, such as excessive use of messaging, printing resources, information storage space, network services or game playing.
3. Accessing, examining, or attempting to examine the files, mail, or account of either other computer users or of system management directories, files, or resources.
4. Accessing, examining or attempting to view, or change the configurations of HLGU’s computers, printers, routers, switches, networks, etc, or any other user’s computers or equipment.
5. Invading the privacy of other individuals or attempting to commit identity theft.
6. Sending, annoying, harassing, or obscene messages. (See Additional Matters Section B)
7. Writing anonymous or pseudonymous communications, which appear to dissociate you from responsibility for your actions, impersonate others and are inappropriate.

8. Using resources for commercial activities including but not limited to commercial solicitation of business. See MOREnet for more information: http://www.more.net/content/service-policies
9. Distributing passphrases or otherwise attempting to evade, disable, or "crack" passphrase or other security provisions.
10. Damaging, modifying, or unauthorized relocation of any University hardware or software.
11. Deleting any University-provided software or deleting any data not belonging to the user without proper authorization.
13. Installing unauthorized software. (See Additional Matters Sections, E, F & G)
14. Introducing a computer virus or other destructive program.
15. Violating any rules or regulations posted.
16. Accessing materials from the Internet including but not limited to pornography and other questionable materials that are not consistent with HLGU's mission in maintaining a Biblical worldview.
17. "Loaning" your account name and passphrase to others.
18. Using sounds or visuals that might distract or offend others.
19. Using network resources for libel, slander, fraud, misrepresentation or any illegal activity.
20. Using or distributing the University's or anyone's logo, seal, trademark or copyrighted materials without prior approval. (See Additional Matters Section D)
21. Any other act deemed illegal under local, state or Federal law.

II. Official Communications

HLGU may send official communications by a variety of means including but not limited to: email, U.S. Mail, text messages, learning management system, the University portals, and apps.

HLGU has the right to expect that students and employees will read the communications in a timely fashion. A person's failure to read official University communications in a timely manner does not absolve the person from knowing and complying with consent of the official communication.

FERPA

All communications, including protected information, will be consistent with local, state, and federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA). To ensure compliance with FERPA regulations, all correspondence which concerns protected information should utilize official HLGU communication methods that best align with appropriate security measures. See HLGU's FERPA Policy for further details at https://www.hlg.edu/academics/registrar/ferpa/

Email

An HLGU email account is only issued to employees, registered students, campus groups and affiliated individuals. The HLGU address will be listed as the official email address in the student or employee's record. Users are encouraged to only use their HLGU email address for work or school related purposes. HLGU will not be responsible for the handling of email sent or forwarded to outside service providers.

Students give HLGU permission to send FERPA protected information to a non-HLGU email address if they do any of the following:

a. Initiate a message from a known address,
b. Respond to an official HLGU message via their alternate email address, or
c. Provide an alternative email address.

HLGU does not condone auto-forwarding to non-HLGU email accounts. This helps to mitigate the chance that protected data is not inadvertently released.

Data Retention or Recovery

HLGU may outsource some or all of its email services and is not responsible for email retention or recovery. In addition to the University policies, students and employees will be required to agree to and be bound by the vendor's terms of use. Campus constituents are strongly encouraged to maintain a backup of important email and documents. See the Document Retention Policy for more details.

HLGU Mass Email Privileges and Responsibilities

Mass email to the entire student body is reserved for official University use only. Individuals may maintain and send to their own group listings for classes, clubs, friends, etc.

Only designated roles approved by the Executive Cabinet receive mass email privileges for campus email groups. See the Office of Computer Services Mass Email Procedure for more details.

Employees should not use mass email except for official University business and as is necessary to perform their job duties. Employees may also not use mass email for solicitations, non-HLGU fundraisers, advertisements of personal items for sale or for partisan purposes.

III. Legal Responsibilities

In addition to the ethical responsibility of the computer user, there are also legal responsibilities. By using the HLGU network, Wi-Fi, or other computing resources, users agree to abide by the terms set forth in this policy. This Agreement is entered into by the parties in the State of Missouri, and the laws of the State of Missouri shall determine all questions pertaining to the construction and validity of this Agreement. Any cause of action or lawsuit brought under this contract shall be filed only in Marion County, Missouri. Those using HLGU network, Wi-Fi or other computing resources agree to indemnify Hannibal-LaGrange University for any and all costs associated with any breach of this agreement including but not limited to damages, judgment interest, court costs, and attorneys' fees.

Federal law has established penalties for infringements upon copyrights, intellectual property rights, and privacy rights of individuals. The Revised Statutes of the State of Missouri Sections 569.095-569.099 have established penalties of tampering with intellectual property of computer users or computer equipment. Individuals may be convicted of a felony with penalties ranging from a one-year sentence and a fine of $1,000 to a five-year sentence with a $5,000 fine, depending on the damage caused. Federal penalties may include imprisonment and fines up to $250,000. In addition, RSMo. 537.525 allows for civil penalties and attorney’s fees be charged against offenders.

The guidelines presented here reflect U.S. Copyright Law, DMCA, State of Missouri Statutes, and additional specific rules imposed by the University. These statutes can be found in various locations on the internet. Please ask the library staff for help in locating any of these laws.

For information on fair use guidelines please visit
https://www.copyright.com/education-campus-guide-to-copyright/copyright-basics/

IV. Disciplinary Procedures

Inappropriate use of computing services and facilities will not be tolerated and may result in loss of computing privileges. Disciplinary action will be pursued for violation of these codes and statutes through appropriate University procedures.

Violations may result in disciplinary and/or legal action and may result in loss of access, fines, probation or other disciplinary actions through the Office of Student Life or appropriate supervisor.

Computer use privileges may be suspended immediately upon the discovery of policy violations. Suspected violations will be confidentially reported to the appropriate authority. Violations will be dealt with in the same manner as violations of other University policies. Disciplinary reviews will consider a full range of sanctions including, but not limited to, warnings, the loss of computer use privileges, dismissal from the University, and legal action including referral to State and Federal prosecutors. Violations of some of the above policies may result in criminal prosecution and the filing of civil lawsuits to recover damages and attorney fees.

V. Additional Matters

A. Privacy and Protection: Users should not expect any measure of privacy concerning information stored on or passing through HLGU’s network. Due to circumstances beyond HLGU’s control, viruses, vandalism, etc. can cause information to be distributed to anyone. Furthermore, the network administrators may access files, email, etc. as needed for maintenance, to answer inquiries from proper authorities, or other purposes. Upon separation from employment, supervisors and/or replacement may have access to all email and all files that the former employee had stored or access to. Please be advised due to the US Patriot Act, law enforcement agents can access files without a subpoena. Information posted on the internet including social networking sites are publicly accessible, and care should be taken on what is posted.

A limited amount of privacy is provided by assigning users logins and passphrases which normally prevents one user from accessing the account of another user. Even the best of computer systems cannot protect the individual who fails to conceal his or her passphrase. Leaving a computer without logging off is like leaving the door of your home unlocked and open. Using an obvious passphrase is like hiding your door key under the doormat. Users are responsible for all activities done using their account. Users should change passphrases regularly and not share them.

Important work should be stored and backed up regularly. Even so, not all data may be able to be restored. HLGU limits the amount of time certain data is kept. Please see the Data Retention Policy for details.

Multi-factor authentication (MFA), also known as 2FA or two-step verification, is required for access to various HLGU services.

B. Harassing messages: Users must refrain from sending any messages with racial, sexual, or other negative overtones. (The messages you send will not only be from you, but from HLGU. Be sure that what you provide for public reading on Internet is something that is not contrary to the mission, goals, policies, and perspectives of Hannibal-LaGrange University.) In addition, forwards or other good-natured messages may be annoying or harassing to some people, so please be considerate. You may have good intentions in sending these types of messages, but sending them to other people may cause problems.

C. Copyright questions: Any questions or complaints regarding copyright registration should be referred to the Library Public Services Technician at 573-629-3137. Library staff can also assist in determining where to request permission for copyrighted materials. Permission to use HLGU logos, seal or other HLGU copyrighted materials should be requested from the Office of Marketing and Communications at 573-629-3118. Unauthorized distribution of copyrighted materials, including peer-to-peer file sharing, may subject those involved to loss of network privileges, disciplinary action, civil or criminal liabilities. See section III & IV for more details.

D. Intellectual property: Questions regarding intellectual property ownership of items developed at or for Hannibal-LaGrange University for instructional use should be referred to the Office of Academic Administration at academics@hlg.edu or 573-629-3092. Questions regarding non-instructional materials should be referred to the Office of Marketing and Communications. Contact the Marketing Coordinator at 573-629-3118 for suspected intellectual property violations done by or through the school.

E. Software authorization: Software should not be installed unless it has been approved by the Office of Computer Services. Requests for authorization may be submitted to ithelpdesk@hlg.edu. Personnel from the Office of Computer Services may delete any unauthorized software found and disciplinary actions may be brought against the party responsible for its installation. In the event of a denial, written appeals may be submitted to the Technology Committee at any time.

F. Peer-2-Peer Networking: Software for Peer-2-Peer Networking such as Bit Torrent, Transmission, WinMX, and Direct Connect is not allowed on computers belonging to the University or accessing the University network, including student computers in dorms. Having this software may result in the loss of network privileges or other disciplinary action.

G. Inspection: HLGU reserves the right to inspect computers if violation of this policy is suspected.

H. Personal Devices: If users bring their own device, services are limited to public Wi-Fi access on campus and the Ethernet in campus housing. HLGU is not required to provide technical support for privately owned devices.

I. Remote Access: Cloud-based services are available to designated users as appropriate and in accordance with vendor licensing agreements. For example, students, faculty and academic staff may have access to the learning management system, but contracted housekeeping staff would not.

> Remote access to library services is limited to HLGU employees and students only.
>
> Remote access to the HLGU network is a privilege granted to a limited number of individuals who have a demonstrated need to perform mission-specific activities while off-campus.

J. Information Security Incidence:
In the case of suspected thefts involving data or exposures (including unauthorized access, use, or disclosure), individuals should provide a description of the incident to the Office of Computer Services (OCS) by either emailing ithelpdesk@hlg.edu or calling 573-629-3032. Upon receipt of a report, OCS staff will investigate the alleged incident. If an issue is identified, the Computer Services personnel will follow the appropriate procedure as listed in the incidence response plan. Depending upon the severity of the compromise, other entities such as the Department of Public Safety, Marketing Department or local law enforcement may be involved.

In the case of a confirmed incident, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of HLGU, that site will be contacted to have the information removed as soon as possible.

K. Printing: Printers are available in most buildings from networked devices. Wireless printing is not available. Students are provided a printing allowance each semester. Beyond that students may pay for additional printing.

Disclaimer:

The Office of Computer Services will do their best to support users in accordance with this policy. Due to various reasons such as not following this policy or recommended procedures or not using university provided tools, OCS may not be able to support the user.