Student Technology Use & Information - CamelNet Connection Privilege Agreement

Computer and network information resources are for the use of Campbell University students, faculty, and staff and are only for the educational, academic, research, and business purposes of the university. Campbell University reserves the right to alter access, availability of access, and the terms of this agreement at any time for any reason.

The use of university information resources is governed by the policies and regulations as outlined in this document and those regarding student conduct found in the Student Handbook. Violations of these regulations will be reported to the appropriate dean and/or department with appropriate disciplinary action to be taken.

Under no circumstances are users of university information resources authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing university-owned resources or conducting university business. The following activities are prohibited. The lists below are by no means exhaustive, but rather attempts to provide a framework for activities, which generally fall into the category of unacceptable use.

<u>Students may not do the following:</u>

1. Download or Distribute Unlicensed Content or Software.
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" content or software products that are not appropriately licensed for use by the university and/or the end user.

2. Share Your Password.
Revealing your account password to any other person or entity or allowing the use of your account by any other person or entity (e.g., administrative assistants, graduate assistants, co-workers, student workers, classmates).

3. Effect Security Breaches.
Accessing data which the User is not an intended recipient or logging into a server or account that the User is not expressly authorized to access unless these duties are within the scope of the User's regular university job function.

4. Disrupt Network Communications.
Interfering with network communications through disruptive activity for malicious purposes (e.g. network sniffing, network floods, packet spoofing, denial of service, and forged routing information).

5. Install Wireless Broadcasting Devices.
Such devices include, but are not limited to, wireless routers and access points. These devices will be confiscated, and the student may lose their network privileges if found in violation of this policy.

6. Circumvent Access Controls.
Bypassing user authentication or authorization access control mechanisms to access or alter university information resources the User is not authorized to access.

7. Grant Unauthorized Access.
Granting access to university information resources to unauthorized Users.

8. Attempt to Intercept, Compromise, or Tamper with Passwords.
Copying password files, password "cracking," installing keystroke logging software, intercepting network traffic, or attempting to discover passwords of other Users to gain unauthorized access to university information resources.

9. Unauthorized Scanning of Networks or Systems.
Scanning University networks or systems for security vulnerabilities (including port scanning) is expressly prohibited.

10. Monitor Network Traffic without Permission.
Executing any form of network monitoring which will intercept data not intended for the User's own computing device.

11. Interfere with Network Traffic.
Using any tools, or sending messages of any kind, with the intent of interfering with or disabling regular network traffic.

12. Interfere with Normal Service Operations.
Intentionally interfering with or denying service to any computing device (for example, denial of service attack).

13. Intentionally Downloading Malware.
Introducing malicious programs into university networks or systems (e.g., viruses, worms, Trojan horses, etc.).

14. Download or Sharing Inappropriate Content.
Displaying, procuring, or transmitting material that is in violation of university codes of conduct, sexual or discriminatory harassment policies or laws, or hostile workplace laws.

15. Using Peer-to-Peer File Sharing Applications.
Using peer-to-peer file sharing applications or websites to upload and/or download and/or share protected intellectual property (e.g., copyrighted video, music, software).

16. Use of the University Network to Engage in Illegal and/or For-Profit Ventures.
Software piracy, copyright infringement, e-mail abuse, cryptocurrency mining, and other illegal activities are prohibited. Any known abuse may be investigated by law enforcement officials. Using university resources to support personal business interest(s) is prohibited.

17. Engage in Harassment.
Any form of harassment via email, telephone, text messages, messaging applications, or other messaging systems, whether through language, frequency, or size of messages.

18. Send SPAM.
Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material

19. Forge Emails.
Unauthorized use, or forging of, email or message header information.

20. Distribute Chain Emails.
Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.

21. Unauthorized Sharing of Email Address Information.
The unauthorized sharing of university email address information with external individuals or organizations is prohibited.

Student Responsibilities Regarding Technology

Students must respect the priority of academic use of the university network. Students are personally responsible for any activities originating from their network connection.

Students are responsible for their personal computer hardware and software. Students must maintain updated virus protection. Students are encouraged to contact the Helpdesk if they need help choosing and/or installing a subscription-based antivirus program.

All computers, regardless of operating system (OS), must be set to receive Automatic Software Updates from the OS manufacturer.

If a student has reason to believe another user or group of users is interfering with access to the University network, they must report the problem to the Student Life and Christian Mission Office. Campbell University administrators will investigate and, if necessary, take corrective action.

Students should avoid representing themselves in any way as agents of the university or using the university's name in a manner that would imply an endorsement of the personal views or activities by the university.

Campbell University assumes no liability for data loss or equipment damage related to a student's use of the university network. Precautions for natural disasters are the student's responsibility. The owner of a computer/device connected to the university network is responsible for the behavior of all Users of that machine and for all network traffic to and from the machine. Campbell University reserves the right to monitor traffic through any data connection for the purpose of checking compliance with this agreement.

By connecting a computer to the CamelNet network, students agree to abide by the terms and conditions set forth above. Students must signify that they have read and will abide by the terms of the Campbell University Acceptable Use Policy and must accept this policy to use the university network.

Technology Usage

The University reserves the right to monitor the use of institutionally owned resources. Alleged inappropriate use of technology resources will be investigated. In instances of misuse, appropriate disciplinary action up to and potentially including legal action, will be taken. Copies of the Acceptable Use Policy are included in official University publications including, but not limited to, the graduate and undergraduate catalogs, staff/faculty/student handbooks, and selected course syllabi.

Eligible Users

Only the following properly authorized people may access Campbell University computing facilities and information resources:

- Undergraduate and graduate students currently active in Campbell University programs
- Non-degree seeking and special students currently active in Campbell University programs
- Campbell University faculty (including full and adjunct), staff, and administration
- Designated alumni
- Official guests of the President and the University
- External constituents accessing library resources
- Individuals formally associated with the University, upon verification of the appropriate dean and/or administrator

Original Work by Students Using University Technology Resources

Original works created by students using Campbell University technology resources are the property of the creator. With the notable exceptions of the processes normally associated with grading, critique, assessment, and lecture or classroom illustrations, no other student, faculty, and/or staff member may make any use of another's work without the expressed consent of the creator. However, the academic department and the university retain the right to display, copy, replicate, and/or distribute any work created using the department's production facilities for the purposes of promotion, representation, artistic display, publication, illustration, and recruiting, on the condition that the creator is given full, appropriately disclosed credit. No one, including the creator, may use the department's production facilities for any commercial purpose.

User Privacy

E-mail and other information passing over the University network, including information stored in user accounts and computers, is private and confidential. Although this type of information must be accessed by IT system personnel for the purpose of backups, network management, etc., the content of user files and network transmissions will not be viewed, monitored, or altered without the express permission of the user except in the following circumstances:

1. The university has reason to believe that an account or system has been

compromised and is being used by someone other than the authorized user.
2. The university has received a complaint that an account or system is being used to gain unauthorized access or to attempt to gain unauthorized access to another network site.
3. The university has reason to believe that an account or system is being used in violation of university policy or federal or state law.

Under these circumstances, Legal Counsel, or the Chief Information Officer or CIO-designated individual may authorize IT support personnel to monitor the activities of a specified account or computer system and to search electronic information stored in that account. The authority for this search must be requested on an account-by-account basis, and monitoring will be restricted to the specified account. If this search provides evidence of violation, the account will be disabled, and action taken with appropriate authorities.