Status Active PolicyStat ID 17107179

Origination	02/2025	Owner	Brandon Seymore
Last Approved	02/2025	Area	Information Technology
Effective	02/2025	Applicability	Bucknell University
Last Revised	02/2025		
Next Review	02/2027		

APPROPRIATE USE POLICY (AUP)

Purpose:

Bucknell University's technology resources exist to support the academic and administrative activities needed to fulfill the university's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully. This policy defines the boundaries of "acceptable use" of University technology resources, including computers, networks, electronic mail services and electronic information sources, as detailed below. By using University electronic information systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable University policies, as well as applicable State and Federal laws and regulations.

Scope:

This policy applies to all users of technology resources owned, managed or otherwise provided by Bucknell University. Individuals covered by this policy include, but are not limited to faculty, staff, students, alumni, and others with access to the University's technology resources and/or facilities as defined by this policy.

Definitions:

"**Technology Resources**" includes all Bucknell owned, licensed or managed hardware and software, email domains, and related services and any use of the organization's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

"**User**" means any individuals granted access to Technology Resources as defined by this policy.

Policy:

Acceptable Use of University Technology Resources

Use of Technology Resources is a privilege extended to members of the University community to fully participate in academic endeavors, research and employment responsibilities. All Users are obligated to use and access Technology Resources in accordance with the standards and obligations set forth in this policy.

A. **Privileges and Responsibility When Accessing University Technology Resources :** Use of Technology Resources is authorized so long as such use does not negatively impact university computer systems, networks, related equipment or otherwise interfere with university business activities and is not prohibited by this or other policies.

    1. Account holders and authenticated Users must safeguard the reliability and security of information Technology Resources and are personally responsible for their use of their University accounts.

    2. Users must maintain a secure and confidential password and ensure the continued security and privacy of the account.

B. **Prohibited Use of University Information Technology Resources:** Technology Resources may not be used in any manner prohibited by state and federal laws, or disallowed by licenses, contracts or University policy. The following uses, while not all inclusive, are strictly prohibited and constitute violation of this policy:

    1. Publishing, posting, transmitting or otherwise making obscene or legally objectionable content available. The University cannot protect individuals against the existence or receipt of material that may be offensive to them.

    2. Using Technology Resources to defame, harass, intimidate, threaten, or discriminate or retaliate against any other person(s).

    3. Sharing any account credentials or allowing another to use any account(s) associated with the University. Use of someone else's credentials for any university service(s) is also prohibited.

    4. Using Technology Resources to violate federal, state or local laws or regulations or university policies. This includes the illegal use of non-licensed software or other material in violation of copyright law or the illegal download of digital content in violation of the Digital Millennium Copyright Act (DMCA).

    5. Providing, assisting or using University systems and networks to gain unauthorized or inappropriate access to University computing resources or systems at remote sites.

    6. Denying or interfering with or attempting to deny or interfere with services to other Users by means of "resource hogging", distribution of computer worms or viruses, etc.

    7. Knowing or reckless distribution of unwanted email or other messages..

8. Using computers located in public areas of the University are for purposes other than academic/research purposes and incidental personal use. Electronic mediums such as games, chat, instant messaging, social networking, recreational movies or TV shows displaying obscene images are prohibited.
9. Using Technology Resources to violate the privacy of others. Viewing, monitoring, copying, altering, or destroying any file, data, transmission, or communication not explicitly owned by the User is prohibited without explicit permission by the owner.
10. Forging, maliciously disguising or misrepresenting your personal identity. This policy does not prohibit Users from engaging in anonymous communications, provided that such communications do not otherwise violate this policy.
11. Using personal network equipment, broadcast points (such as wireless access points or ad-hoc computer-to-computer networks), access points or any device found to be interfering with official University wireless networks.The University may disconnect service or otherwise terminate any unauthorized device without notice.
12. Removing any security controls installed on University equipment.
13. Using personal accounts to conduct University business.
14. Using Technology Resources for commercial purposes or personal gain.

User Privacy When Accessing University Technology Resources

Users accessing Technology Resources have no expectation of privacy for communications transmitted or stored on Bucknell's resources. The University may access, review, monitor, and or disclose information associated with an individual User's account in response to a judicial order or any other action required by law or permitted by official Bucknell policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the university, including but not limited to re the investigation of violations of law or University policy, or when access is considered necessary to conduct University business due to the unexpected absence of an employee, or to respond to health or safety emergencies.

Use of Personal Devices to Access University Technology Resources and Data

Users who access University systems and data on personal devices remain obligated to protect University data. Any University data on non-university-owned devices must be protected with controls equivalent to controls on university-owned devices. Bucknell reserves the right to add device-inspection capabilities prior to allowing personal devices on the University network.

Reporting Unauthorized Use

Users must immediately report the loss, theft, inappropriate use, or suspicious activity related to University access credentials (i.e. passwords, key cards or security tokens), assets (i.e. laptops, desktops), or other information to the IT Tech Desk.

Non Compliance

A. The University reserves the right to immediately take any action it deems necessary, including disconnection of devices and/or suspension of Users or services, to maintain the stability, security and operational effectiveness of computing and networking facilities and to protect information security, system integrity, and operation continuity.

B. Violations of this policy may be referred to the Division of Talent, Culture & Human Resources or the Dean of Students for consideration in accordance with established administrative / disciplinary policies.

Exceptions

Requests for exception to this policy must be submitted in writing to the Vice President of Library & Information Technology (L&IT), or their designee and must specifically state the basis for the requested exception. Exceptions are reviewed by the Vice President of L&IT Technology or their designee on at least an annual basis. Requests for exception may require additional approval by other University officials based on the specific exception, potential exposure of information or degree of potential risk.

Related Documents: