Information Technology Services

ACCEPTABLE USE POLICY

Contents

1.0 – Introduction

The purpose of the Acceptable Use Policy is to provide guidelines for students, faculty, and staff in the appropriate use of technology resources at John Brown University, thus ensuring the best use of University systems for academic and administrative purposes.

John Brown University invests in technology resources to benefit and enhance the educational and administrative efforts of the University. Individuals who are granted access to these resources are given such access as a privilege to carry out the duties associated with their positions and roles at JBU.

Activities beyond these purposes or outside of the provisions of the Acceptable Use Policy are prohibited and may result in revoked access to technology resources or disciplinary action in accordance with University policies and procedures. If any student or employee creates any liability on behalf of JBU due to reasonable knowledge of being in violation of this policy, the student or employee agrees to be fully responsible should JBU need to defend itself against any ramifications of their activities.

All JBU network users are expected to abide by JBU's lifestyle expectations while using the technology resources of the University.

2.0 – Accounts

Students, employees, and approved guests may use University systems through the use of network accounts issued specifically to them. The account holder is personally responsible for the usage of his or her network account. To allow friends, classmates, parents, spouse, children, colleagues, work study, or anyone else to use one's account is to violate the Acceptable Use Policy.

Specific policies include:

2.1 Use only the network accounts, programs, and data that have been authorized for your use.

2.2 Always identify computing work with your own name or other approved ID. Do not attempt to modify files or otherwise work on the JBU network without signing in.
2.3 You are responsible for any activity conducted with your accounts. Do not tell anyone else your password or sign in for someone else using your account. Do not leave a computer unattended without locking it or signing off.
2.4 Assist University security efforts and protect your account by choosing passwords wisely: incorporate mixed-cases, numbers, letters, and symbols; change passwords regularly and often; and do not use obvious names, identities, hobbies, words found in the dictionary, etc.
2.5 Passwords must be at least 10 characters long, must meet certain complexity requirements, and must be changed every 180 days (students), 90 days (faculty/staff), or at more frequent intervals. Whenever a personal password becomes known to another person, that password should be changed immediately.
2.6 Passwords must not be written down in some readily-decipherable form and left in a place where unauthorized persons might discover them.

3.0 – Data and Confidentiality

Any data that is captured, processed, or stored on the JBU network is treated as confidential. This does not imply complete privacy; only that access is limited to individuals authorized by the University. Information Technology Services personnel may access files when necessary to maintain University systems. Every effort is made to respect the privacy of information, but the content of files, email, databases, etc. may be examined at any time as allowed by law.

Specific policies include:

3.1 Information Technology Services is solely authorized to install software on JBU-owned computers. Flexibility is allowed in circumstances where Information Technology Services has granted specific permission, and compatibility and appropriate licensing have been confirmed.
3.2 Use of software owned by the University must abide by the copyright and license agreements associated with the software. Questions about such agreements may be directed to Information Technology Services, but it is the responsibility of the individual person to be familiar with the copyright and license agreements of the given application before using the software. It is illegal to copy most software products.
3.3 JBU computer systems may not be used to download or store illegal copies of copyrighted digital materials, including computer programs, fonts, pictures, clipart and other images, movies and videos, textual information, articles, reports, and music.
3.4 Do not attempt to access, copy, modify, or delete programs or files that belong to other users or the University without prior authorization by Information Technology Services.
3.5 Employees must safeguard privileged and sensitive information to protect University data and the privacy of individuals. Third parties may be given access to internal information only when a demonstrable need to know exists, when such access is in compliance with other relevant legislation (FERPA, HIPAA, etc.), and when such a disclosure has been expressly authorized by the relevant information owner. In particular, sensitive or privileged information should not be released to external media sources, except through University Marketing & Communications and official public relations processes.
3.6 All information on University computer systems should be considered private, unless it has been specifically classified otherwise. Any attempt to circumvent computer or network security in order to gain access to private information is considered a violation of the Acceptable Use Policy and may be illegal.
3.7 The internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the internet may be at risk of detection by a third party. You should exercise caution and care when transferring such material in any form.

4.0 – Email

It is a University expectation that all students, faculty, and staff will use their University email account for all email communication to and from University offices and officials. Email messages are normally retained until deleted by the recipient, but once an account has been terminated, email may not be retained unless required by law. John Brown

University cannot make any guarantee, explicit or implied, regarding the privacy of electronic mail. Occasionally, University personnel may see all or part of an electronic message during routine system maintenance. Every effort is made to respect the privacy of email, but the content of email messages may be examined at any time as allowed by law. Information contained in electronic messages may be used against you in disciplinary proceedings.

Student email accounts will remain enabled for one year after active enrollment. Employee email accounts will be closed after the last day of employment.

Specific policies include:

4.1 JBU email accounts are the property of both the University and the individual. Do not harvest or distribute JBU email addresses for use by any third party.
4.2 Only authorized personnel are allowed to send bulk email messages with approved academic or administrative content to University email recipients. Do not send email messages to large distributions on the JBU address list without prior authorization. Personal solicitation through JBU email is prohibited, including: promoting political or social causes, creating and forwarding "chain letters", forwarding "junk mail" to individuals not specifically requesting it, and sending email using forged addresses or headers.
4.3 Electronic communication is vulnerable to interception, misdirection, or rerouting. Therefore, highly confidential materials should not be delivered via email.
4.4 Email users are assigned storage quotas and are expected to check their JBU email messages frequently and remain within quotas. Delete unwanted messages. Email mailboxes are not intended to be used for extended storage and file attachment archival purposes.
4.5 Electronic mail, web pages, and other electronic resources are for University related activities. Sending or storing harassing, threatening, sexually explicit, or offensive material is not allowed on University resources and may result in disciplinary action.
4.6 Email messages sent from university accounts are considered privileged and confidential and may not be forwarded or copied to third parties without express authorization by the sending party. In particular, email messages may not be released to external media sources, except through University Marketing & Communications and official public relations processes.

5.0 – Network and Internet

JBU utilizes network and internet resources that are limited, expensive, and shared by many different people. Students, faculty, and staff should show consideration in their use of these resources by refraining from monopolizing systems, overloading networks with unnecessary or excessive data, and wasting printing supplies and other resources.

Students in campus residences may connect personal computers and approved devices to the network from their rooms and are expected to abide by all of the policies contained in the Acceptable Use Policy in their use of network resources and the internet.

Employees connect to the network using University-owned computers to do University-related work. Employees may connect personally-owned computers and devices to the JBU private network when key technical and procedural protections are in place, such as a valid JBU network account to provide appropriate authentication. See section 6.0 – Personal Computers.

Specific policies include:

5.1 Consult with Information Technology Services before connecting or enabling a personally-owned network device (i.e. router, Wi-Fi printer, Wi-Fi range extender) to the JBU network. These types of devices should not be connected or enabled, since they may conflict with other University technologies, reduce internet bandwidth, or cause significant network issues.

5.2 Do not attempt to disable or bypass network security systems. This includes the use of various "tunneling" protocols and proxy servers to hide the true nature of what you are doing.
5.3 Intentional compromise of system integrity by malware or other means may result in disciplinary action. Do not attempt to modify system facilities in any way.
5.4 JBU-provided network storage should be used for University academic and administrative work. You should not use JBU network space to store personal files, including personal digital pictures, music, and video files.
5.5 Attempts to access pornographic, sexually explicit, gambling, or other materials deemed inappropriate by JBU's lifestyle expectations may be blocked, logged, and reported. Students and employees who show evidence of intentional access to such materials are subject to disciplinary action.

6.0 – Personal Computers and Devices

Students, faculty, and staff may connect personally-owned computers and devices to the JBU private network given certain requirements and provisions. Connections are available in campus residences, specific labs, and wireless zones around campus. Any data created, accessed, or stored on the JBU network using personally-owned computers and devices is subject to the same policies and guidelines as data created, accessed, or stored through the use of University-owned computers and devices.

Specific policies include:

6.1 All personal technology usage that makes use of JBU network and technology resources must be done in accordance with acceptable use guidelines and JBU lifestyle expectations.
6.2 Your computer should be running a supported operating system version and the available security patches and updates should be up-to-date.
6.3 Your computer should be running a current anti-malware program with updated signatures.
6.4 You should do JBU work-related tasks on University-owned computers to insure compatibility of software, compliance with license agreements, and optimal security.
6.5 JBU makes no guarantee for the security or safety of your computing device when connected to the network. ITS makes every effort to keep the network secure, but we still cannot completely control what other people bring to the network.
6.6 You are responsible for the activities of other people using your computer, including roommates, spouses, and children.
6.7 If your computer or network device is identified as the source of a problem on the network, it may be disconnected without notice.
6.8 Information Technology Services is unable to provide comprehensive support for personally-owned computing devices, other than to provide reasonable guidance to utilize technology resources within the context of the JBU network.

7.0 – Recreational Use

Personal and recreational use is secondary to the primary academic and administrative purpose of University network resources. JBU recognizes, however, that there are legitimate times when students and employees use the network for recreational purposes. A significant number of students live on campus and benefit from recreational use of the network. Faculty and staff may have occasional need to engage in personal correspondence and research activities as long as such activity does not interfere with expected job performance.

Specific policies include:

7.1 All personal and recreational use must be done in accordance with acceptable use guidelines and JBU lifestyle expectations.
7.2 Use of University technology and support resources for personal, taxable income generation is prohibited outside of faculty scholarship and other University-approved activities meeting acceptable use guidelines.

7.3 Bandwidth-intensive activities that compromise use of the network for academic and administrative priorities may be blocked or significantly limited.
7.4 Refrain from running recreational programs, such as games, on University computers unless specifically authorized as part of an academic or University-approved exercise.
7.5 File sharing must only include materials for which a person has legal ownership.
7.6 JBU reserves the right to revoke personal-use privileges if such use is found to be in conflict with an individual's employment responsibilities.
7.7 JBU reserves the right to deny network access to anyone found in violation of these provisions.

8.0 – Acknowledgement

The Acceptable Use Policy may change without notice and changes in policies will supersede or eliminate those documented in any printed copy. The authoritative version of the policy will be online: https://info.eaglenet.jbu.edu/policies/aup.pdf.

9.0 – Revision History

Date	Description
August 2018	▪ Wording update in policy 4.2 regarding the promotion of political/social causes.
February 2019	▪ Minor wording changes; password policy updates.
March 2019	▪ Updates to password policy information.
May 2019	▪ Comprehensive review with additions and wording changes.
July 2019	▪ Minor wording changes.
November 2020	▪ Email policy clarification 4.6 added.