Acceptable Use of Technology Resources Policy

Effective Date:	Last Updated:	Prepared by:	Approved by:
3/31/19	7/1/09	Timothy Hopkins	Miroslava Mejia Krug

1. Purpose

To help foster and protect the technology environment for the promotion of teaching, learning, research, business, and service, Benedictine University requires all users of its technology resources to comply with standards of academic and professional ethics, University codes of conduct and policies, and all applicable laws and regulations.

This policy details the University's ownership and monitoring of its Technology Resources, as well as the requirements for obtaining access to, and proper usage of those resources by Authorized Users. This policy applies to all persons and all devices accessing or using any Benedictine University information system or service.

2. Definitions

A. Authorized Users: Students, faculty, staff, emeriti, invited guests, contractors, agents, and all other persons granted authorized access or user privilege.

B. University IT Resources: University owned, operated, leased, licensed, or contracted networks, telephones, systems, and services, whether local or hosted, individually controlled or shared, including:

- Wired and wireless networks
- Student and staff information systems and databases
- University provided email accounts and services
- Networked and local storage systems and devices
- Telephone and other communication systems
- Accounts operated by the University, including social media and other hosted platforms
- University data maintained in electronic format

In addition to this policy, users of University IT Resources agree to abide by the rules and regulations contained in applicable guidelines and policy and procedure manuals, as well as state and federal laws, including but not limited to those dealing with:

- FERPA
- HIPAA
- GLBA copyright infringement
- Defamation
- Discrimination
- Fraud
- Harassment
- Identity theft

3. Policy

Benedictine University recognizes that free expression of ideas is central to the academic environment. For this environment to flourish, all users must adhere to this policy.

Benedictine University voluntarily provides technological resources. The primary purposes of these resources are to meet the academic, research, administrative, and communications needs of its students, faculty, and staff. The use of these resources for other purposes is tolerated provided that usage is kept to a minimum and does not violate [a] any federal, state, or local law, [b] the University mission or policies, and [c] guidelines or rules stipulated in this policy. Users who make incidental personal use of University Technology Resources do so at their own risk. The university cannot guarantee the security or continued operation of any Technology Resource.

Access to any Benedictine University owned and/or operated technology resource is a privilege and not a right. Individuals who refuse to follow the Acceptable Use Policy will not be granted user accounts or may not be granted access to services/systems. Violations of this policy by individuals with accounts may result in penalties including but not limited to closure of all accounts and revocation of all privileges. Other penalties may be levied up to and including dismissal from the University or termination of employment.

4. Confidential Data

All users are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of confidential data and ensure that no unauthorized disclosures occur. All users must refrain from sharing confidential data with anyone not authorized to view or possess such data. All users must comply with the provisions of the Benedictine University Confidentiality Agreement and all federal/state/local privacy laws and regulations, including GLBA and FERPA.

5. University Ownership/ Monitoring

Technology Resources are the property of the University. The University’s ownership of a file, record, data or a message does not transfer ownership to the University of any intellectual property therein. Incidental personal uses are permitted as provided in this policy and are included in the definition of Technology Resources for the purposes of University access and use. Records of electronic communications pertaining to the business of the University are considered Technology Resources.

The Provost or the cognizant Vice President may grant access to the account of an Authorized User to other University employees or designated individuals when specifically authorized in writing, as long as the request includes the following:

1. What access/user account is being requested?

2. Why is this being requested? and

3. Who is going to access this information and for what duration?

The University President, Chief of Staff and Counselor to the President, General Counsel, or Chief Information Officer may also provide written authorization to grant access following the procedure set forth herein.

6. Expectation of Privacy

All technology resources, including email accounts and shared storage, are provided by Benedictine University in furtherance of its mission. No representation has been made to Users as to the privacy of any communication or data stored on or sent through Benedictine University technology resources. Users should have no expectation of privacy while using the University network or any technology resource. Email and files that are sent, received, or stored using University resources are the property of the University. Email is not a secure form of transmission. Benedictine University reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove or otherwise alter any data, file, or system resource which may undermine the authorized use of any computing facility or which is used in violation of University rules or policies. Benedictine University also reserves the right periodically to examine any system and any other rights necessary to protect its computing facilities.

The University may monitor the activity and accounts of Users of Technology Resources, with or without notice, when:

A. The user has voluntarily made them accessible to the public, as by posting to a blog or a web page;

B. It is necessary to protect the integrity, security, or functionality of University or other Technology Resources, or to protect the University from liability;

C. There is reasonable cause to believe that the user has violated, or is violating, this Acceptable Use Policy, or other University policies or guidelines, or laws or regulations;

D. An account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns; or

E. It is otherwise required or permitted by law.

Any such monitoring, other than of information made available voluntarily or necessary to respond to emergency situations, must be authorized in advance by the University President or the University’s Legal Counsel after consultation with the University President. If such monitoring is of the University President, then it must be authorized in advance by the University's Legal Counsel.

The University, in its discretion, may also disclose the results of such monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies, and may use those results in appropriate University disciplinary proceedings.

Under certain circumstances, the University may access and modify the contents of an email account. In cases concerning the health, safety or welfare of the University community, as determined by senior University officials, the University may authorize accessing or modifying an employee's email account. In cases where personally-identifiable information may have been inappropriately disclosed, University officials may authorize modification of the email accounts of both senders and recipients.

The Benedictine University computing and Technology Resources constitute a private system. As such, the information stored on University owned or contracted equipment is the property of the University with the exceptions noted in the Creative Works section of the Faculty Handbook.

The University may use software tools to block electronic content and shape network bandwidth. These tools, such as Anti-Spam, Anti-Virus, and Firewalls, will be used to ensure the security of the technology environment. Web sites and Internet services may be blocked if they are known to spread viruses, spyware, adware, or other types of malicious software or service, harm or attempt to harm any University Technology Resource, or illegally host copyrighted material made available for download.

User Responsibilities

Users are responsible for all activity that happens on their accounts.

All users must:

- Maintain the privacy and security of all data;
- Keep passwords confidential;
- Comply with all information security policies and procedures;
- Be responsible for the data stored on his or her system, or in a shared network drive, by ensuring backups are maintained and controlling access, when appropriate;
- Adhere to all laws and regulations regarding copyright and intellectual property;
- Report any security incident or suspected misuse of any technology resource to the Chief Information Officer or designate.

All users must not:

- Install software or use any computing device in any way that degrades the network or makes inaccessible any other technology resource for any user;
- Share passwords with anyone or otherwise grant access to another person (except IT personnel) to their own account, computer, or other resource provided by the University;
- Obtain extra electronic resources or access to accounts for which they are not authorized;
- Misuse, alter, or otherwise damage any computer equipment;

- Engage in any activity designed to spy on network traffic or to access other users' accounts, passwords, files, or programs;
- Display or cause to display pornographic, obscene, abusive, racist or inappropriate material at any public or employee workstation or digital display. The University reserves the right to judge the appropriateness of displayed material;
- Install unlicensed or “pirated” software;
- Install software on a student-accessible computer (with the exception of Information Technology staff);
- Use University technology resources to relay mail;
- Install network or other technology hardware (including wireless access points, hubs, switches, etc.) without prior written authorization from the Chief Information Officer. Unauthorized equipment will be confiscated;
- Use any technology resource to support political or non-University related business interests;
- Represent the University on social media or by any technology means unless authorized to do so
- Disable, remove, or uninstall software designed to provide a secure computing environment, including patches of existing software, on any institutional information system without prior approval from IT.
- Sell, rent, or provide access to University technology resources to outside individuals, groups, or businesses except as authorized by the Chief Information Officer for authorized University business relationships

7. Enforcement

Benedictine University retains unfettered discretion to monitor, authorize, control or stop the use of said technology at its sole discretion. Alleged violations of the Acceptable Use of Policy will be referred to the Vice President of Student Life (students), the Provost (faculty), or the Vice President for Administration and Finance and Chief Financial Officer (non-faculty employees) for investigation and action through the established disciplinary processes of the University. Violations of this policy may result in disciplinary action up to and including expulsion or separation from the University, and may also result in legal action. In addition, the University may:

- Delete files or programs;
- Inactivate user access privileges;
- Remove the user account.

If a user believes that her or his rights have been violated by another user of University technology resources, the user should report the incident to the Vice President of Student Life (students), or her or his supervisor (faculty and staff) for appropriate action.