Berry College

Policy on the Acceptable Use of Information Technology Resources and Data

I. Purpose

This policy provides guidelines for the appropriate use of technology resources and data at Berry College. This includes information and data in any electronic format and any hardware or software to create, process, transmit, store or use such information/data. This may include computers, networking systems (including wireless), databases, digital information/images, electronic mail, messaging, servers, applications, storage devices, telephones, wireless devices and web sites.

II. Scope

Berry College information technology resources as defined above are owned by the college and must be used in support of the college's mission. Users of those resources on campus or off campus, include, but are not limited to, students, faculty, staff, contractors, visitors, visiting scholars, prospective students, camps and conferences attendees, and guest speakers.

III. Policy

General Guidelines

In support of the College's mission of teaching, service, and work, the Office for Information Technology provides computing, networking, and information resources to the college community. Users are responsible for using these resources in an effective, efficient, ethical and lawful manner. All existing laws (local, federal and state) and college regulations and policies apply, including not only those laws and regulations specific to computers and networks, but also those that may apply generally to personal conduct. Using Berry College's Internet access and electronic communications services means that one has read the acceptable use policy and agrees to abide by the guidelines.

Acceptable and Ethical Use

The use of Berry resources is granted to authorized users primarily for education, research, service and administration. Berry College encourages an environment in which ideas can be freely exchanged along with a commitment to academic freedom. It is the user's responsibility, however, to practice the following:

- Comply with all federal, state, and other applicable laws; college policies and procedures; and all contracts and licenses.
- Respect and honor the rights of others regarding intellectual property, privacy, freedom from harassment, academic freedom, copyright and use of IT resources.
- Make regular backups of information and files as appropriate and to store those backup files in a secure location.
- Regularly delete files from one's accounts on shared computing resources (i.e., file servers or "shared drives") according to campus or departmental retention policies.
- Maintain the confidentiality, security and availability of computer systems and information on all devices under their control to prevent loss, theft, damage or inappropriate disclosure.
- Properly secure all mobile devices with sensitive data (FERPA, HIPPA, etc.) and encrypt all files per the guidelines in the Mobile Computing Policy.
- Never share passwords with others and use only the passwords and privileges associated with your account and for the authorized purpose. Users must respect the privacy of other users and their accounts, regardless of whether those accounts are properly protected.
- Monitor access to accounts. If unauthorized activity is suspected, users should report it to the technical support desk and change the password immediately.

• Use college provided software in a manner that abides by licensing provisions, including installation, use, copying, number of simultaneous users, and other license terms.

Misuse of Resources

Users are accountable for their conduct under all applicable college policies and procedures. Misuse of computing, networking, or information resources may result in the loss of computing privileges and could result in prosecution under applicable statutes. Complaints alleging misuse of campus computing resources will be directed to the Provost (faculty), Vice President of Student Affairs (students) or the Vice President for Business and Finance (staff) for review. In each case, the vice president will investigate the alleged misuse and render a determination with sanctions, if appropriate. Illegal reproduction of software protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment. Activities will not be considered misuse when authorized by appropriate college officials for security or performance testing.

Examples of misuse include, but are not limited to, the following activities:

• Using a computer account or password other than one's own. Never share your computer account or disclose your password to anyone.

• Using the campus network to gain unauthorized access to any computer or network.

• Performing an act which interferes with the normal operation of computer systems or networks.

• Knowingly running or installing on any computer system or network, or giving to another user, a program intended to compromise, damage or place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, remote access Trojans, worms, and malware.

• Attempting to circumvent data protection methods or uncover security vulnerabilities.

• Violating terms of applicable software licensing agreements or copyright laws. This includes the downloading of copyrighted material such as audio and video files for which the copyright owners have not granted rights.

• Intentionally accessing, downloading, uploading, receiving or sending materials that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent or defamatory language, except for officially approved and/or legitimate academic purpose.

• Masking the identity of an account or machine.

• Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

• Using the college's electronic mail and/or equipment for solicitation, political communication, advertising, or for any commercial purpose unrelated to official college business.

• Connecting and operating unauthorized wireless access points, switches and/or routers on the campus network.

Email Use

Berry email is an official means of college correspondence. All students, faculty and staff should check their email on a regular basis, preferably at least once per day. It is the responsibility of all faculty, staff and students to properly maintain their email account. Email accounts may remain active for students for life. Employee accounts will be deactivated on the last day of employment or at a later date if the employee has made arrangements with the Office for Information Technology. Retirees may request to keep email accounts.

Personal Use

Berry College permits occasional and reasonable personal use of its Internet and email services provided that this does not interfere with work or educational performance. These services may be used outside of normal work and academic scheduled hours, as long as such use is consistent with professional conduct.

Preservation of Electronic Data

Federal and state laws exist which mandate the preservation of data, including communications and documents stored or transmitted in electronic format, in certain circumstances. The college may be

legally obligated to preserve data when it is directly or indirectly related to a subpoena, a request for production, or it is relevant to any possible issues where litigation or court process may be involved. This may include electronic communications and any other documents stored or transmitted in electronic format. All users are required to comply with requests from the Office of General Counsel, outside counsel, and/or the Office for Information Technology, by cooperatively assisting in the identification and preservation of such data to the greatest extent possible. Failure to comply and cooperate with such notices and requests, and/or willfully or knowingly obstructing or hindering the gathering and preservation of such data in any fashion, may subject the College to sanctions and increased liability. This will be considered a violation of this policy and subject the user or users to discipline.

Privacy

Berry College affirms that the mutual trust and freedom of thought and expression essential to the academic mission of a college rests on an expectation of privacy, and that the privacy of those who work, study, teach, and conduct research in a college setting be respected. The college respects the privacy of all electronic communications, but users should have limited expectations of privacy regarding metadata while using Berry College owned or leased equipment and services. The normal operation and maintenance of the college's technology resources require backup and caching of data and communications, logging of activity, monitoring of general use patterns, and other such activities necessary to provide and protect service. Therefore, information technology administrators collect metadata—such as file storage/space allocation, bandwidth usage, and data and email statistics—on an ongoing basis to ensure the integrity and reliability of the college's electronic network.

As is the case for information in non-electronic form stored in college facilities, the college's need for information will be met in most situations by simply asking the author or custodian for it. Consistent with this policy, the college reserves the right to access, review and release electronic information transmitted over or stored on college systems or facilities. Properly authorized college officials, following the guidelines below, may access relevant e-mail, voice mail, or electronic files without the consent of the assigned user upon a good faith belief that such action:

- Is necessary to comply with legal requirements or process, or
- May yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected serious infraction of college policy (for example alleged research misconduct, plagiarism or harassment), or
- May yield information needed to deal with an emergency, or
- In the case of Staff, will yield information required for the ordinary business of the college to proceed.

If a need arises to review or access electronic files of employees or students, requests must receive approval from the Provost (faculty requests), the Vice President of Student Affairs (student requests), or the Vice President of Business and Finance (staff requests). Procedure:

1. Requests should be directed to the Chief Information Officer (CIO).
2. The CIO will seek approval from the Provost or appropriate Vice President as designated above and will advise the requestor as to the approval or denial.
3. If approved, the CIO will forward the request to the Assistant CIO/Director of Network Operations for fulfillment.
4. The Assistant CIO may request other IT staff to fulfill the request, but staff involvement will be kept to a minimum to maintain confidentiality.
5. It will be assumed that the request has been made without the knowledge of the subjects of the request. When appropriate, an attempt will be made to notify the user of this access in advance.
6. The Assistant CIO will report the findings back to the requesting party. A summary of the findings and any pertinent notes will be sent to the requesting party, the approving party and the CIO.

Except as may otherwise be dictated by legal requirements, individuals will be notified of access to, or disclosure of, the contents of their e-mail, voice mail or their computer accounts as soon as practicable.

In cases where such notification might jeopardize an ongoing investigation of suspected wrongdoing, it may be delayed until the conclusion of the investigation.

Copyright Policy and Notification Procedures

The owner of a copyright holds exclusive rights to the reproduction and distribution of the copyrighted work. Duplication of any copyrighted work is prohibited unless specifically allowed for in a license agreement. Unauthorized copying of intellectual work and/or software is illegal and punishable under federal law.

As members of the academic community, we value the free exchange of ideas; however, respect for the intellectual work and property of others is essential to the mission of all educational institutions.

Copyright Infringement Notification – Agent to Receive Notification of Claimed Infringement

This is to notify copyright owners that the agent to receive infringement statutory notices under the Digital Millennium Copyright Act is Tom Hocut, Assistant CIO and Director of Network Operations.

A copyright owner needing to send such notice to Berry College should submit the notice in writing to: Tom Hocut Berry College P.O. Box 495035 Mount Berry, GA 30149 E-mail: thocut@berry.edu Phone: 706-236-5099

For more information about copyright, see www.whatiscopyright.org or libguides.berry.edu/copyright.

IV. Compliance/Sanctions

Any user of Berry College technology resources who violates the acceptable use or other college policies or applicable local, state, or federal laws may be subject to appropriate disciplinary actions up to and including termination of access, disciplinary review, expulsion, termination of employment, legal action or other appropriate disciplinary action. Schools and departments shall not adopt rules that reduce full compliance with applicable local, state, or federal laws or the policies and procedures of the college.

V. Approval and Review

This policy is periodically reviewed by Information Technology staff and the Information Technology Committee. Recommendations for major changes or additions to this policy will be referred to academic council and administrative council for approval. Information technology resources and systems are changing rapidly and the college reserves the right to amend this policy at any time.

Record of Changes

Date	Version	Action	Action Taken by	Notes
4/17/2014	1.0	Issued	CIO – Penny Evans-Plants	Approval Date Unknown, but posted as official
7/11/2018	1.0	Reviewed	DirInfoSec – Dan Boyd	Past-due review
7/11/2018	1.1	Revised	DirInfoSec – Dan Boyd	Updated and revised, awaiting approval
7/17/2018	1.2	Revised	DirInfoSec – Dan Boyd	Further revision, awaiting approval
7/19/2018	1.2	Approved	General Counsel & CIO	No further approval needed
7/25/2018	1.3	Modified	DirInfoSec – Dan Boyd	Minor change – removal of links