Acceptable Use Policy

Effective Date:	March 1, 2010
Revised Date:	January 14, 2026
Department:	Information Technology
Former Title:	Fair, Responsible, and Acceptable Computer Use Policy
Administration:	Chief Information Security Officer

PURPOSE

The purpose of the acceptable use policy (AUP) is to define the standards and expectations for the responsible, ethical, and legal use of Butler University's information technology resources. This policy aims to protect the security and integrity of technology systems, ensure compliance with all relevant laws and regulations, and promote a safe and productive environment for all users. By adhering to the AUP, users contribute to the overall effectiveness and security of Butler's IT infrastructure.

POLICY STATEMENT

1. Fair & appropriate use cases of Butler technology resources include:

    a. Supporting the mission of the University: teaching/learning, creative activities, research, or engaging Butler constituents

    b. Supporting studies, instruction, duties as employees, official University business, and University sanctioned activities

    c. Incidental personal use

2. Individuals covered by this policy must:

    a. Comply with all University rules and policies

    b. Comply with all federal, Indiana, and other applicable laws and all applicable contracts and licenses. Users must use institutional information technology resources only for lawful purposes, and not for any purpose that is illegal, immoral, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission and values of the University, or likely to subject the University to harm.

    c. Use only those information technology resources they are authorized for use and use them only in the manner and to the extent authorized.

    d. Observe the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Accounts, passwords, and access to University information technology resources may not, under any circumstances, be shared with, transferred to, or used by, persons other than those to whom they have been assigned by the University.

    e. Respect the finite capacity of information technology resources and limit use to the extent needed for authorized activities, so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

        i. The University may require users of information technology resources to limit or refrain from specific uses in accordance with this principle. The University will judge the reasonableness of any particular use in the context of all of the relevant circumstances.

    f. Comply with the law with respect to the rights of copyright owners in the use, distribution, or reproduction of copyrighted materials.

        i. The University is also required by law to investigate claims of possible copyright infringement taking place through its computer networks. Internal University sanctions for unauthorized use or distribution of copyrighted material range from warnings to the loss of privilege to use University information technology resources.

g. Store university data only in University-approved secure locations and handle data according to the university Data Policy.

h. Promptly report any confirmed or suspected security incidents to the Information Technology department.

3. Subject to the Privacy of Personally Created Content Policy, the University reserves the right to inspect any activities or accounts of individual users of University information technology resources, including individual login sessions and communications, without notice, unless otherwise prohibited by law. The University may inspect such information technology resources under circumstances when the University determines inspection is necessary, including but not limited to the following:

    i. To protect the integrity, security, or functionality of University or other information technology resources, or to protect the University from harm;

    ii. There is reasonable cause to believe that the user has violated, or is violating, any Butler policy or applicable civil or criminal law; or

    iii. An information technology resource appears to be engaged in unusual or unusually excessive activity, as indicated by monitoring of general activity and usage patterns.

    b. The University, in its discretion, may use or disclose the results of any such inspection, including the contents and records of individual communications, as it considers appropriate to University personnel, third parties, or law enforcement agencies.

4. Individuals covered by this policy must **not**:

    a. Use information technology resources for commercial or personal purposes, for personal financial gain (except as part of a class sponsored activity), or as primary computer systems for an outside organization.

        i. The University permits occasional non-commercial personal use of Butler's information technology resources. Such use should not consume a significant amount of those resources, interfere with job performance or other University responsibilities, interfere with the efficient operation of the University or its information technology resources, and must be otherwise in compliance with this Policy.

ii. The University assumes no responsibility for the loss or recovery of personal files.

iii. Exception may be made where approval has been granted from college/division leadership and Information Technology and applicable accounts obtained in advance.

b. Use University resources to post, view, print, store, or send obscene, pornographic, sexually explicit, or offensive material, except for officially approved, legitimate academic or University purposes.

c. Circumvent security measures at Butler or on other networks.

d. Engage in any activity intended to cause harm to University systems or data, information, or files contained therein.

e. Impersonate others.

SCOPE

This policy applies to all users of university technology and associated services including but not limited to faculty, staff, students (current, prospective, and former), affiliates, contractors, vendors, and volunteers.

This policy does not alter or supersede individuals' or the University's rights or obligations to comply with applicable federal and state laws or regulations governing the use and privacy of information, including:

- Family Educational Rights and Privacy Act (FERPA),
- Gramm-Leach- Bliley Act (GLBA),
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), and
- Payment Card Industry Data Security Standard (PCI-DSS).

EXCEPTIONS

N/A

ADMINISTRATION

This policy shall be reviewed at a minimum, every three years, or when the following conditions occur:

- Security policy changes occur within IT
- University policy changes regarding the roles and responsibilities
- Federal guidelines regarding data change

RELATED POLICIES

- Technology Master Policy
- Privacy of Personally Created Content Policy
- Confidential Information Policy

REVISION HISTORY

- Revised/renamed by the CISO and Approved by University Cabinet on January 14, 2026
- Revised by the Chief Information Officer, April 7, 2020
- Annual review by CISO, January 23, 2019
- Approved by the Board of Trustees: February 26, 2010
- Approved by Sr. Administrative Group: January 19, 2010
- Approved by the Information Management Council: December 20, 2009
- Created 12/20/2009 as complete rewrite from Computer Use Policy, June 2002