Privacy of Personally Created Content Policy

Effective Date:	March 1, 2010
Revised Date:	January 14, 2026
Department:	Information Technology
Administration:	Chief Information Security Officer

PURPOSE

This policy affirms and protects the privacy rights of all individuals affiliated with Butler University—including students, faculty, staff, affiliates, and others with Butler network access—regarding content they create during their affiliation with the University. It outlines the safeguards for such individually created content and specifies the processes by which others may request and obtain access to that content.

POLICY STATEMENT

1. Personally created content stored on Butler systems will only be accessed by:
    a. The account holder
    b. Automated systems intended to prevent data loss or misuse
    c. The assigned user of a device or system, except in the limited cases outlined in this policy
2. This policy applies to all digital assets created or modified during a person's affiliation with the University, including but not limited to:
    a. Files, email, and voicemail (stored, encrypted, or in transit)
    b. Content in University-owned or managed cloud services (e.g., OneDrive, LMS, Email, Voicemail, Teams)

c. Data on University-owned computers and related technologies assigned to individuals or groups
d. University data and files stored on personally owned devices

3. Authorization for Access
    a. Written authorization is required before university personnel may access a user's files or systems, except in situations outlined in Section 4.
    b. Standard Authorization Process
        i. Approval from (1) the Chief Information Security Officer (CISO) or a CIO-designated alternate and (2) one of the following**:** the President, applicable Executive Vice President, applicable Vice President, or applicable College Dean.
        ii. If the request concerns the President, written authorization must also be provided by the Chair of the Board of Trustees.
    c. Requests from the Office of the General Counsel
        i. When actual or anticipated litigation requires review of a user's files or systems by internal or external counsel, any request to access, review, preserve, or collect user files or system data must be initiated by the Office of the General Counsel and approved in advance by (1) the Chief Information Security Officer (CISO) or a CIO-designated alternate and (2) the Vice President and General Counsel.
    d. Standing Authorizations:
        i. The CISO may grant ongoing, narrowly scoped authorization to specific IT personnel for critical operational needs, data loss prevention, or emergency incident resolution.
        ii. All such access must be documented and reported to the CISO promptly.

4. Situations Not Requiring Written Authorization
    a. Access may occur without formal approval when:
        i. Collaborative resources are inherently non-private (shared folders, group devices)
        ii. System-generated information is needed for maintenance, performance, or security
        iii. Network monitoring is performed to maintain network security and reliability
        iv. User-requested assistance is provided (implied consent)
        v. Routine administrative work such as backups, upgrades, or troubleshooting is performed

5. Permitted Reasons for Access Without User Consent
    a. Permitted reasons may include but are not limited to:
        i. Critical operational necessity (user unavailable or incapacitated)
        ii. Reasonable cause for investigation of potential legal or policy violations
        iii. Data loss prevention (suspected exposure of sensitive information such as PII, PCI, HIPAA, FERPA)
        iv. Compliance with legal demands (subpoena, warrant, or court order)

v. Request from family or estate of a deceased student or employee
vi. Prevention of substantial University risk of harm or liability
vii. Security incidents, malware containment, or forensic data preservation

6. Procedure for Accessing and Reviewing Data
    a. Request Submission – Initiated via IT Help Desk
    b. Approval – CISO (or CIO in their absence) secures necessary authorizations
    c. Data Review – Limited to the minimum number of individuals needed to fulfill the purpose
    d. Findings – Account holder may request a summary of findings, when appropriate
    e. Notification – Users will be notified before access whenever feasible, unless:
        i. Notification risks data alteration/destruction
        ii. The user is no longer affiliated with the University
        iii. Urgency makes prior notice impractical
        iv. Circumstances make prior notice inappropriate

7. Ownership of Data After Termination
    a. Any files or data left on Butler devices after termination of employment become the property of Butler University.

8. Recordkeeping
    a. IT will maintain a confidential log of all requests for access to data or systems made under this policy.

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.

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

- Acceptable Use Policy

REVISION HISTORY

- Revised by the CISO and Approved by University Cabinet on January 14, 2026
- Reviewed by the CIO, April 20, 2020
- 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