Docusign Envelope ID: 682E3E14-0CA6-4806-9CE1-C13AFDD6B7E9

CHEYNEY UNIVERSITY OF PENNSYLVANIA
IT-2025-011426.04: ACCEPTABLE USE POLICY

Vetting Channel: This policy was originated by the Office of Information Technology (OIT) with oversight from Division of Administration and Quality Control. The enforcement area for this policy is a collaboration between Office of Information Technology, Human Resources, Dean of Student Affairs and university campus community.

History of Edits:

Adopted Date: 01-05-26 Effective Date or Semester: Spring 2026

Amended Date: 01-14-2026 Effective Date or Semester: Spring 2026

Related Policies:

- FERPA Policy
- File Data Sharing Policy

Additional References:

- U.S. copyright law (Title 17, U.S. Code)
- The Digital Millennium Copyright Act (DMCA) data protection, and information security.

I. Purpose

The purpose of this policy is to promote responsible, ethical, and secure use of Cheyney University's computer systems, networks, and digital resources. These resources exist to support the institution's mission of teaching, research, learning, and community service.

II. Scope

The scope of this policy applies to all computers, servers, mobile devices, and networked equipment owned or managed by Cheyney University. It also includes all users of IT resources owned or operated by Cheyney University of Pennsylvania. It also applies to all use of university provided internet, email, cloud services, and academic technology platforms.

III. Definitions

IT resources
include the university computer network, all university-owned (operated, serviced) devices, and all university-provided software systems regardless of what computer network is being used. This is inclusive of all content transmitted over the university computer network by any device regardless of ownership.

Personally Identifiable Information (PII)
The National Institute of Standards and Technology (NIST) defines as any information about an individual, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Docusign Envelope ID: 682E3E14-0CA6-4806-9CE1-C13AFDD6B7E9

Security Breach

When an unauthorized person gains access to sensitive, protected data or systems, bypassing security controls, leading to theft, exposure, or disruption

Users

To include faculty, staff, students, contractors, vendors, any third-party consultant, affiliates, and guests, who access the university's network or computing resources, equipment or connecting resources.

IV. Policy Statement

Use of the university's IT resources is a privilege and signifies agreement to comply with this policy. Users are expected to act responsibly and follow the university's policies and any applicable laws related to the use of IT resources. This policy provides regulations to ensure that IT resources are allocated effectively.

The university recognizes the role of privacy in an institution of higher education and will endeavor to honor that ideal. There should be an expectation of privacy of information stored on or sent through IT resources utilized through the university. However, there are instances required by law where disclosure of information may be required. For example, the university may be required to provide information stored in IT resources to someone other than the user because of court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-to-Know statute (65 P.S. 67.101 et seq.). This type of request must be responded to in a timely manner, contingent to the requestor's specification.

Information stored by the university may also be viewed by approved technical staff working to resolve technical issues. As this policy applies to contractors, vendors and affiliates, these third-party entities are responsible for the protection of PII, the acceptable use of IT resources and meet all standards set by the university for record retention, non-personal identifiable information and laws associated with information requests. Third party associates are also responsible for reporting security breaches to the Office of IT as soon as a breach is discovered.

V. Responsibility

Authorized users are expected to:

- Respect the intellectual property of authors, contributors, and publishers in all media.
- Protect user identification, password information, and the system from unauthorized use.
- Use university computing resources for legitimate educational, research, and administrative purposes.
- Respect the privacy and academic freedom of other university users.
- Protect individual login credentials and report any suspected security breaches or account misuse immediately to the Office of Information Technology by emailing the Helpdesk at helpdesk@cheyney.edu
- Follow all applicable laws and institutional policies regarding U.S. copyright law (Title 17, U.S. Code) and the Digital Millennium Copyright Act (DMCA) data protection, and information security. Upon the Office of IT being in receipt of a DMCA notice, the Office of IT will take the

Docusign Envelope ID: 682E3E14-0CA6-4806-9CE1-C13AFDD6B7E9

initial investigation and will take appropriate action, including disabling network access or notifying the user and appropriate university personnel.

- Comply with federal, state, and local laws, relevant university personal conduct regulations, and the terms and conditions of applicable collective bargaining agreements. Applicable laws include, but are not limited to, those regulating copyright infringement, copyright fair use, libel, slander, and harassment.
- Use university email which is the official university communication and official collaboration tools for academic or administrative communication.
- Secure sensitive data (e.g., student records, research data, HR information) in compliance with FERPA, HIPAA, and other regulations.

Unacceptable Use

Users must not:

- Access or attempt to access systems, data, or accounts without authorization.
- Use university resources to engage in harassment, discrimination, or hate speech.
- Install or use unlicensed software or applications that compromise system security.
- Use the network for commercial gain, illegal activities, or political campaigning (unless authorized under institutional policies).
- Interfere with network performance or security, including the use of unauthorized wireless access points, VPNs, or file-sharing services.
- Send spam, phishing, or any mass unsolicited messages.
- Engage in academic dishonesty or plagiarism facilitated by technology.

Database, Network and System Security

All devices connected to the university network must comply with institutional security standards, including up-to-date antivirus protection and operating system updates. The IT department may monitor network traffic, log activity, and restrict access to maintain performance and security. When users suspect malware, data breaches, or lost/stolen devices, they should report it to the IT Help Desk.

Administrative access to servers and databases is restricted to authorized personnel only.

Data Privacy and Confidentiality

The university respects the privacy of users' personal communications and academic work; however, it reserves the right to monitor and review system activity when necessary for maintenance, security, or legal compliance. Sensitive information, including student records (FERPA), health information (HIPAA), and financial data (GLBA), and Cheyney's Safeguard Rule must be handled according to university data governance and privacy policies. Users should avoid storing sensitive data on personal devices or unapproved cloud platforms such as DropBox. Data

Docusign Envelope ID: 682E3E14-0CA6-4806-9CE1-C13AFDD6B7E9

can only be stored on Cheyney University-approved devices, systems, and platforms to protect the security, confidentiality, and integrity of all customer information entrusted to the University.

Internet, Email, and Social Media Use

Internet and email resources should primarily support academic and administrative functions. Limited personal use is acceptable if it does not interfere with university operations or violate this policy. Employees may make incidental personal use of IT resources in compliance with the Acceptable Use Standard for Information Technology Resources and other University policies and standards but cannot interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment.

Email communications must be professional and consistent with the university's standards of conduct. Official university communications must be sent from institutional email accounts.

Users should exercise good judgment and academic integrity when posting or sharing information on social media platforms.

Enforcement

Questions regarding the applicability or violation of the policy, or appropriate access to information, should be referred to the appropriate (divisional) Executive Leadership Member. Violations of this policy should be reported to and investigated by the Office of Information Technology to determine appropriate technical actions, including but not limited to the denial of services. IT will then report an infraction to the Office of Human Resources for university employees or the Dean of Student Affairs for students. Criminal violations will be investigated by the Campus Police and referred to the Pennsylvania State Police, if necessary.

Acknowledgment

All users are expected to understand and comply with this policy when using university technology.

Date Received from the Committee or Policy Proposer(s) to Division Chief:	
Date Received from Division Chief to ELG/COT:	
Division Chief's Approved Signature:	Signed by: ronald Williams 8B8C335B2FF2425... 1/15/2026
Date Reviewed by ELG or COT: (circle the decision-body)	
President's Approved Signature:	DocuSigned by: Aaron A. Walton 1/15/2026 BEGDC83B89DB484...
Policy Number Assigned:	IT-2025-011426.04