# ACCEPTABLE USE OF INFORMATION TECHNOLOGY

**POLICY NO.: CU-IT-40**

## Section 1. General

1. **Scope:** This policy applies to all students, faculty, staff, volunteers, third party contractors, and anyone else using information technology resources owned and/or operated by the University. Concord University's Information Technology (IT) resources are provided to support the academic and administrative functions of the institution.

2. **Authority:** W. Va. Code §18B-1-6; §18B-2A-3.

3. **Effective Date:** TBD

4. **Purpose:** It is the policy of Concord University to provide access to University Information Technology to carry out the mission of the University. This policy outlines acceptable use standards and responsibilities for all users of Concord University's Information Technology (IT) systems and services. Access to such IT resources is a privilege that comes with expectations of ethical conduct, responsible behavior, and adherence to applicable laws and University policies. This policy ensures that IT resources are used safely, securely, and in a manner that protects institutional data and user privacy.

## Section 2. Responsibility

1. All users are expected to maintain the security, integrity, and confidentiality of institutional information while using these shared resources responsibly. Users must adhere to the legal and ethical standards governing copyright, software licensing, and intellectual property. Users of the university's information technology resources are expected to utilize them in a responsible manner by taking proper care of these resources, providing reasonable security, reporting known or suspected technology breaches, and respecting the property and privacy rights of others.

## Section 3. Acceptable Use

1. Users must have an authorized University account. Credentials (usernames and passwords) are confidential and must not be shared or used to impersonate others.

2. IT resources must be used in ways that support the University's educational, research, and service missions. Personal use must be limited and must not interfere with university operations.

3. Users must adhere to all federal and state laws, rules and policies of the Higher Education Policy Commission and Concord University, including copyright, privacy, and intellectual property laws.

4. The University provides the following principles to users regarding responsible and acceptable use of IT services and resources:

    a. All University Technology services and resources are considered to be State resources and services as the University is a state entity.
    b. Use of such resources implies consent to this Policy and all IT policies.
    c. Any employee who wishes to engage in research that may violate this policy must obtain approval from both the Provost and Chief Information Officer (CIO) before engaging in said research. Requests for such must be submitted in a timely manner to allow for proper review.
    d. An Authorized User is someone who has been granted a username and password and, if applicable, has been granted access to use the resource(s).

**Section 4. Violations**

1. The following is a non-exhaustive list of violations and prohibited conduct with respect to acceptable use of the University's IT resources and services:
    - **a.** Unauthorized access, modification, or destruction of data.
    - **b.** Use of IT resources for commercial gain, fraud, or personal profit.
    - **c.** Harassment, threats, or distribution of offensive materials.
    - **d.** Use of peer-to-peer file-sharing software unless explicitly authorized.
        i. Peer-to-peer file sharing is the distribution and sharing of digital media using peer-to-peer (P2P) networking technology. P2P file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content.
    - **e.** Misuse of University branding, digital identity, or domain names.
    - **f.** Disclosure of confidential or personally identifiable information (PII) to unauthorized parties.
    - **g.** Furnishing false or misleading information or identification in order to access another user's account.
    - **h.** Using another person's username/password or letting someone else use your username/password.
    - **i.** Investigating, reading or attempting to access another user's files without permission.
    - **j.** Monitoring the electronic communications of others.
        - **i.** This includes, but is not limited to, intercepting emails, virtual meetings, phone calls, and video calls that the user was not privy to receive.
    - **k.** Attempts to access or manipulate certain components of the information technology environment without authorization.
    - **l.** Alteration of software, data, or other files without authorization.
    - **m.** Disruption or destruction of equipment or resources.
    - **n.** Avoiding being charged for computer resources including the unauthorized use of another user's account.
        - **i.** This includes, but is not limited to, unauthorized use of Adobe Creative Cloud, Google Cloud, and Amazon Web Services.

**o.** Copying or attempting to copy data or software without authorization.
**p.** Sending email or a program which will replicate itself or do damage to another user's account.
**q.** Interfering with legitimate work of another user.
**r.** Sending abusive, harassing, pornographic, or obscene messages through use of the University's IT services, including the internet.
**s.** On shared computers such as in computer labs, excessive recreational use of resources that prevents academic use by those waiting for an available computer.
**t.** Sharing protected personal identifiable information (PII) data with unauthorized external entities such as in email, Artificial Intelligence, or unsecure storage.
**u.** Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network.
**v.** Transmitting phishing, hoax, forged, and/or other malicious messages, including messages sent under someone else's username.
**w.** Any activity or action that violates the University's Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws.

**Section 5. Reporting Violations**

**1.** Suspected or known violations should be reported to the Chief Information Officer (CIO) or the Chief Operations Officer (COO) as soon as possible.

**2.** If anyone using Concord University resources, at any time, suspects an attempt to scam a university account by using such compromising schemes as phishing, ransom for fee, spoofing, Ponzi, identity theft, ATM/debit/credit card, telemarketing, charity, or any other fraudulent attempts, must immediately report the attempt to the CIO or COO.

**Section 6. Enforcement and Sanctions**

**1.** Violations of this policy may result in disciplinary action including, but not limited to, suspension of IT privileges, academic penalties, employment actions, or legal prosecution.
   a. Investigations will be conducted under the supervision of the Chief Information Officer (CIO) in conjunction with the Chief Operations Officer (COO), and may include examination of files, logs, and communications.
   b. Users will be notified of investigations, where appropriate, and given an opportunity to respond.
   c. The university may, at its discretion, deny the use of resources during an investigation or when such usage conflicts with the mission of the University.

**2.** Concord University Technology Services may be authorized to engage in investigations and apply certain restrictions and/or penalties in order to enforce this policy.

**3.** These penalties may include, but are not limited to:
   a. temporary or permanent reduction or elimination of access privileges to any or all of the components of the University Technology Resources, and, if necessary to preserve the integrity of the facilities, services, or data, may suspend access whether or not the account owner is suspected of a violation.

4. Once the threat or potential threat to the university is contained, the CIO and COO will determine if an investigation is warranted or required and every effort will be made to avoid disclosure of any content to anyone other than those with a need to know.

5. Where there are ethical or legal implications Technology Services personnel are instructed to contact the CIO and COO who will authorize its disclosure to appropriate authorities if deemed warranted, including University, State and Federal law enforcement officials.

**Section 7. Privacy and Monitoring**

1. While the University values user privacy, it reserves the right to monitor and access IT systems for legitimate business, legal, and security purposes. Users should have no expectation of complete privacy when using University systems. Use of Concord University resources is a privilege and not intended to serve as a public forum. The University complies with the West Virginia Freedom of Information Act and applicable laws governing access to public records and data.

2. In the course of normal maintenance of the IT environment, certain information may be seen by those attending to the maintenance. All employees of the Office of Technology Services are instructed that the disclosure of this information is a punishable offense (as is willful intrusion without cause) unless the information violates this policy or relevant laws. In this case, the employee is required to report the violation to the CIO.

3. Willful intrusion without cause, for the purpose of this policy, is defined as the intentional and unauthorized entry, interference or seizing or taking possession of another's privacy by bypassing security measures or exploiting vulnerabilities in IT infrastructure to get access to systems that should be accessible only to authorized users.

**Section 8. Appeals**

1. An individual accused of a violation of this policy will be notified and have an opportunity to respond before the final determination of a penalty is made. The CIO, in conjunction with other appropriate, responsible parties (e.g., university counsel, student judicial affairs, academic affairs, or Human Resources) will examine the available evidence and circumstances. If a penalty is levied, the decision may be appealed through designated University processes for faculty, staff and students.

2. In cases where a conflict of interest may exist, or in the absence of the Chief Information Officer, the COO or President of the University will enforce this policy.

**Section 9. Amendments**

This Policy may be amended to change names, titles, grammatical and spelling errors, links to information, and contact information without resorting to the rulemaking process. Federal and State laws, rules and regulations change. Any portion of this policy and process document may be modified in practice to ensure the due process rights of the individuals involved are provided and to conform

with any current Federal and State law, rules and regulations. Subject to the institution's rulemaking policy, the institution will change this policy to conform to the most current laws and regulations within a reasonable time of discovering the change.

**Approval:**

Intent to Plan approved by Board of Governors: **April 15, 2025**
Policy approved by the Board of Governors: