Acceptable Use & Technology Security Policy |

(Last Updated August 2025)

COE COLLEGE

This document outlines the policies regarding use of technology resources at Coe College.

User Responsibilities & Understanding

- Only files to be used for academic, administrative or approved research purposes shall be stored on college-owned computers or servers. In addition, college technology resources (such as email, software, etc) should only be used for academic, administrative or approved research purposes. All college-provided equipment and technology services are the property of the college.
- Employees are only permitted to access technology resources and data directly tied to the functions of their job description.
- Electronic mail (Gmail) will not be used to send abusive, obscene or otherwise harassing communications in accordance with the Campus Civility Statement. (Located in the College and Employment Policies Handbook and in the College Policies and Student Handbook.)
- Computer and network facilities are provided as a shared resource for all users. No user shall use College computing and network resources in such a way as to interfere with the ability of others to use them.
- Respect Intellectual Property: The use of campus computer resources to share or distribute copyrighted material to others without the permission of the copyright holder is prohibited. This includes, but is not limited to, using peer-to-peer applications to share these files. The burden of proof of ownership or obtaining permission from the copyright owner is upon the account holder. Upon receiving proper notification, as defined by the Digital Millennium Copyright Act, of a potential infringing activity, we will where possible remove or block access to the material in question.
- Security of the computer systems is in place to ensure resource availability to all users. No user will seek to penetrate or intentionally circumvent the security of any campus communications network or computer system.
- Users are not permitted to attach wireless routers or wireless printers to the College network.
- Students and faculty are expected to keep an active Coe College (coe.edu) email account and to keep in mind that the administration, faculty and various offices at the College will send both official and unofficial communications to them by email. Users are prohibited from setting up coe.edu email accounts to automatically forward outside of the coe.edu domain.
- A user's account is the responsibility of the user.
- Sharing passwords is prohibited and the requirements outlined in the Password Policy, including use of MFA, must be followed.
- Password storage/management best practices should be followed. This includes use of a password management system or other method of tracking such as a password vault on a cell phone. Passwords should not be saved in a Google doc or spreadsheets (this not only includes Coe passwords but passwords for other websites or systems). Passwords should not be written down and left in a visible/easily found place (ex - taped under a keyboard, on a whiteboard/bulletin board, etc).
- Passwords/passcodes should not be reused across unconnected systems. The password/passcode used for the main Coe password (myapps.microsoft.com, gmail, etc) should not be used for other Coe systems or for personal use. (For example: Your Coe password should NOT be the same password used for your social media accounts or banking accounts.)
- Software will not be copied or used illegally. Installation of software should be vetted through IT and follow the Software Request Policy.
- No technology resource will be used for an unsanctioned commercial purpose.
- College-managed lab/podium computers are regularly wiped. Therefore users should not save information directly on the local hard drive/desktop of these devices.

- All college equipment such as laptops, desktops and servers, are required to employ Full Disk Encryption.
- Screen lockout policies are required on all college-owned computers. Mobile devices should be secured following the Mobile Device Security Policy.
- Data and technology policies are available to users on My Coe and should be reviewed and complied with (My Coe > Employee > Data & Technology or My Coe > Student > Information Technology). These policies include but are not limited to:
    - Computer Lab Usage Policy
    - Technology Purchases & Replacement Policy
    - Network File and Storage Policies
    - Separated Employee's Network/Email Account Policy
    - Separated Student's Network/Email Account Policy
    - Software Request Policy
    - Mobile Device Security Policy
    - Password Policy
    - Employee Work from Off-Campus Technology Policy
    - Identity Authentication Policy
    - Red Flag Rules
    - Privacy Policy
    - Third Party Processors (Data Usage) Policy
    - Internal Data Requests Policy
    - Records Management Policy
    - Reporting Data Breaches & Incidents
- The Office of Information Technology follows a variety of documented procedures to contribute to the security of Coe's network. This includes but is not limited to a Change Management Policy & Procedure, Technology Platform/Account Access Policy & Procedure and Patching, Upgrade & Testing Procedure for Technology.
- The Office of Information Technology routinely shares information and training regarding technology security best practices. Users are expected to review this information and ensure they understand it. Employees with certain elevated levels of access may be required to complete additional technology security training. All employee training requirements can be found in the Employee Technology Training Policy. In addition, students are required to complete annual training distributed by the college.
- Users should note that operating system/software updates are pushed to college-owned computers at 1:00 AM on Wednesday mornings, on a weekly basis. Users should make an effort to leave their computer on campus and on during this time period.
- Users should note that 4 AM - 7 AM on Fridays is reserved for IT system infrastructure updates (My Coe, Moodle, Jenzabar, internet access, etc). Notifications of updates taking place are at minimum posted on My Coe.
- When using Artificial Intelligence through systems such as large language models, generative AI systems, machine learning, etc, for security and privacy purposes, users of Coe systems must adhere to this policy overall as well as the below guidelines:
    - **No input of sensitive data. See below for guidelines regarding confidential information:** Users are prohibited from inputting any Coe College managed data or information into AI tools, applications or platforms. This includes identifiable personal, financial, academic, health, sensitive or institutional data as well as confidential organizational information that can be tied to Coe.
        - Users should never input sensitive personal or personal identifiable information (PII) into AI systems unless approved through the Office of Information Technology.
        - Through the college's licensing, Coe users have access to Microsoft Copilot with "Enterprise Data Protection" and Google's Gemini AI tool with "Enterprise Data Protection." In both cases, Enterprise Data Protection licensing includes security and privacy features. In addition, input data is not used to train the foundational Copilot/Gemini models as it is in other generative AI systems. The enterprise protection only applies when users are logged into Copilot/Gemini using a coe.edu email address and credentials. If you need to input confidential information into an generative AI platform, at this time Copilot and Gemini are the only platforms the college supports for use with confidential information. Please note: "Confidential" does not include sensitive personal or personal identifiable information (PII). Sensitive personal or personal identifiable information

should not be input into any AI tools at this time (this includes your own information as well as information like a list of student, employee or alumni names or contact info). Only de-identified data can be used in these AI platforms.

- **Infringement of intellectual property rights:** You may not use AI tools or services to infringe on copyright or any other intellectual property rights, including but not limited to generating content that replicates or mimics copyrighted works (e.g., music, literature, software, images) without the proper authorization. This includes using AI to produce or distribute content that violates patents, trademarks or trade secrets. Please see the college copyright policy for general copyright information.
- **Misinformation and inaccuracies:** Generative AI may generate responses that are not always accurate or up to date. Users should independently verify the information provided by generative AI, especially when it comes to specific facts or rapidly evolving subjects.
- **Academic use:** Students should refer to their course syllabus for guidance on AI use for academic purposes.

Privacy

- Users should be aware that the privacy of computer use is not and cannot be guaranteed. Although the College does not routinely examine the content of user files on College-owned or College-controlled computer systems, it does reserve the right to do so. Suspicious activity on the network/Coe systems are investigated when alerts are received.
- Users should also understand that the College routinely copies many files on many College-owned and College-controlled computer systems for backup purposes. Security tools scan these copies for vulnerabilities and for embedded code. These copies are retained for some time, and while the College does not routinely do so, it reserves the right to examine the content of these copied files. The College takes steps to protect the data residing on the computers that it owns or controls from unauthorized access. Users should understand that the efficacy of these steps is not and cannot be guaranteed.
- Many software systems are designed to collect usage information and to log user activity. This includes but is not limited to antivirus, firewall and email auditing tools, that all send alerts to the Office of Information Technology. The college routinely aggregates the data stored in these logs for analytical and technology security purposes. In general, the college makes no attempt to extract from the logs data regarding the activity of individual users. The college does, however, reserve the right to do so and will do so for troubleshooting and security purposes.
- For technology security purposes and/or at the direction of the President, the Coe Information Technology Office (and third-party vendors acting at the direction of the Coe Information Technology Office) reserve the right to review logs/suspicious activity and act upon the information for technology security purposes.

Policy Enforcement

All users of the college's computing facilities are responsible for understanding the principles set forth above. Alleged violations of the acceptable use policy will be investigated. Users found to have violated any provision of the policy will be subject to disciplinary action. Such action could include, but may not be limited to, loss of access to college technology resources and/or other college/legal actions.