Email Account Acceptable User Policy
Policy Number

Type of Policy:	Information Technology
Last Revised:	May 4, 2021
Review Date:	May 4, 2024
Contact Name:	Dustin Gardner
Contact Title:	Information Security Officer
Contact Email:	gardnedj@cobleskill.edu
Reason for Policy:	The policy defines and explains expectations and responsibilities for all users of SUNY Cobleskill administered email services, including students, faculty, staff, volunteers, affiliates, retirees, and alumni of SUNY Cobleskill.
Policy Statement:	Users are expected to act with honesty, integrity, and respect for the rights, privileges, and privacy of the College community. SUNY Cobleskill email accounts should be used for institutional purposes only, not personal correspondence (see Privacy and Confidentiality, below). Users are expected to abide by all applicable federal and state laws and rules, including SUNY Cobleskill policies and SUNY regulated policies. Please find the SUNY Cobleskill Conduct Codes at the bottom of this document for reference.

Policy:

Expectations of Appropriate Use of Email

Users are expected to act with honesty, integrity, and respect for the rights, privileges, and privacy of the College community.

SUNY Cobleskill email accounts should be used for institutional purposes only, not personal correspondence (see Privacy and Confidentiality, below).

Users are expected to abide by all applicable federal and state laws and rules, including SUNY Cobleskill policies and SUNY regulated policies. Please find the SUNY Cobleskill Conduct Codes at the bottom of this document for reference.

Ownership/Administration

Faculty/Staff/Volunteers/Affiliates/Retirees/Alumni: SUNY Cobleskill owns all email accounts that exist on systems it administers regardless of its hosting provider. The College does not routinely monitor or restrict content residing on its systems. However, if there is a reasonable cause to believe that a user has violated this policy or other applicable College policies, SUNY policies, and/or federal and state laws and regulations, if there is an immediate threat to account or network security, or the College is compelled to preserve or provide records by competent authority, the College reserves the right to take any of the following actions:

1) Review relevant email communications (see Account Investigation, below)
2) Suspend a faculty or staff member's access to the College's computing and networking resources (temporary or indefinitely); and/or
3) Limit a faculty or staff member's access to the College's computing and networking resources (temporary or permanently); and/or
4) Remove the documents/materials/postings from the College's computing and networking resources.

Students: SUNY Cobleskill owns all email accounts that exist on systems it administers regardless of its hosting provider. The College does not routinely monitor or restrict content residing on its systems. However, if there is a reasonable cause to believe that a user has violated this policy or other applicable College policies, SUNY policies, and/or federal and state laws and regulations, if there is an immediate threat to account or network security, or if the College is compelled to preserve or provide records by competent authority, the College reserves the right to take any of the following actions:

1) Review relevant email communications (see Account Investigation, below)
2) Terminate a student's access to the College's computing and networking resources (temporary or permanently); and/or
3) Limit a student's access to the College's computing and networking resources (temporary or permanently); and/or
4) Remove the documents/materials/postings.

Privacy and Confidentiality

Official College communications sent by email are subject to the same public information, privacy and records retention requirements and policies as other official College communications. All email communications are subject to release under the Freedom of Information Law.

The College will not review governance votes or correspondence unless compelled to do so, nor will the College Administration make any decisions based on votes cast in the process of Faculty Governance.

By using the College's computing and networking resources, users are consenting to monitoring of these resources when policy violations are suspected, when a litigation hold is received, when a security threat is identified, or in other appropriate circumstances without further notice to the user. The College maintains the right to unrestricted monitoring or access to electronic information for compliance, security, investigatory, and disciplinary purposes. In using the College's computing and networking resources, users shall have no expectation of privacy.

Sending Sensitive Content over Email:

Email by nature, is an insecure medium of communication. Messages are sent over a computer network in human-readable (plain-text) format, making the messages and anything inside them vulnerable to interception and misuse by a third-party.

Sensitive information such as Personally Identifiable Information (PII) should never be sent in plain-text inside an email message body or inside an attachment within an email.

If there is a valid business need to send PII or otherwise protected information over email, users should consult with ITS who can recommend or provide a solution to securely send this information to its intended recipient.

Sensitive, confidential, or otherwise protected information should never be sent to any user, especially an individual outside of SUNY Cobleskill, without appropriate identity confirmation and adherence to regulations (FERPA, HIPAA) pertaining to the release of the information in question.

Personal Email Use:

"Personal Email" refers to any email account that is not administered by SUNY Cobleskill.

In the interest of maintaining information security and preventing information disclosure, personal email accounts should never be used to conduct SUNY Cobleskill responsibilities.

Automatic Email Forwarding:

Automatic email forwarding is the process of directing messages received at one email address to another email address automatically. While this function has legitimate uses, it poses an information security and regulatory risk to SUNY Cobleskill. Using automatic email forwarding places potentially sensitive, confidential, or otherwise protected information in the

hands of a third-party email provider with no responsibility to protect it. Third-Party email providers may also reserve the right to collect, distribute, read, or claim ownership to any information residing on their servers, which could place SUNY Cobleskill research in danger.

SUNY Cobleskill faculty, staff, volunteer, affiliate, retiree, and alumni users are never to automatically forward emails to another email address outside of the SUNY Cobleskill email system. If it is discovered that messages are being forwarded from a SUNY Cobleskill email account to a third-party email provider, the third-party email account in question will be immediately blocked from sending/receiving email to/from the SUNY Cobleskill email system. The user will also be instructed to remove any SUNY Cobleskill content from the email address that was being forwarded to.

Multi-Factor Authentication:

Multi-factor authentication (MFA) is a process that requires that the person attempting to access a computer resource provide a one-time code, or positive approval of the login using an out-of-band verification device such as a cellular telephone, landline telephone, or mobile telephone application. SUNY Cobleskill uses MFA as a supplement to strong passwords to more effectively authenticate users and authorize their access to resources such as Email, Office 365 services such as OneDrive and SharePoint, and the campus Virtual Private Network (VPN) connection.

MFA is applied to all student, faculty, staff, volunteer, affiliate, retiree, and alumni accounts deployed by SUNY Cobleskill. It is the responsibility of the SUNY Cobleskill account holder to make appropriate provisions for receiving MFA confirmation codes via SMS text message, audio call, or by downloading the Microsoft Authenticator application. If provisions are not made to comply with SUNY Cobleskill MFA policy, the user will not be able to access protected resources until these provisions are made.

Phishing and Malicious Emails:

Phishing emails are messages designed to trick users into clicking malicious links, download malicious files, or provide their username and password to an unauthorized user. Cybercriminals that send phishing emails are primarily financially motivated and are looking for a way to compromise private network resources to either extort the owner of those resources or exfiltrate valuable data from inside the network systems.

If a user receives an email that seems suspicious, appears outwardly dangerous, obscene, or threatening, they are instructed to forward the message to **ITSCyberSecurity@cobleskill.edu.**

If a user believes that they are a victim of phishing or begins to experience strange activity on their email account, they should immediately contact the **ITS Helpdesk**, or send an email to **ITSCyberSecurity@cobleskill.edu.**

Account Investigation

A Cobleskill.edu email address is subject to investigation if prompted with evidence of a policy or legal violation. The Chief of University Police and the Director of Human Resources will need to approve of the investigation concerning any College account before any data will be collected by ITS. All Investigations will follow appropriate, reasonable protocols and legal/regulatory parameters set forth by SUNY Cobleskill and the State of New York. The investigations will be supported by ITS, by having ITS provide raw data to the Chief of University Police and the Director of Human Resources to evaluate and take appropriate action if warranted. All SUNY Cobleskill accounts, regardless of employment or enrollment status, must follow these guidelines.

Continuation of Email Services Following Retirement/Graduation

Graduates are granted a 6-month grace period after the last active semester at which time the account is automatically disabled. Disabled student accounts are maintained for one year, at which time the network/email account is deleted if student has not officially enrolled for classes. SUNY Cobleskill reserves the right to terminate or disable an account at any time due to College policy or to preserve security of the systems. Students have the option to receive a SUNY Cobleskill Alumni Email account maintained by SUNY Cobleskill prior to the deletion of their student email account. The student will receive instructions and assistance in transferring applicable data from their Student email account to their Alumni email account.

Based on official notification from the Human Resources Office of retirement status, retiring faculty members may submit an appropriate request form with the ITS Office to keep their cobleskill.edu email account.

Violations/Abuses

Direct violation or abuse of the campus policies may result in restriction of access to SUNY Cobleskill's email system and/or other appropriate disciplinary action, including sanctions for students under the Code of Conduct.

SUNY Cobleskill Computer Resources Policy: https://www.cobleskill.edu/about/offices-services/information-technology/resources-policy.aspx

SUNY Cobleskill Conduct Codes: https://www.cobleskill.edu/campus-life/student-conduct/conduct-codes.aspx

Policy History:

Revision Date	Author/Owner	Description of the action on the revision date
5-4-21	Dustin Gardner	Policy Update