BRIDGEVALLEY COMMUNITY & TECHNICAL COLLEGE

EMAIL ACCOUNT POLICY

Date approved by cabinet: March 8, 2023
Effective date: April 20, 2023
Expiration date (5 years from effective date if not renewed): April 20, 2028

Section 1. Purpose

1.1. The purpose of this policy is to establish the guidelines for the use of the electronic mail services (email) at BridgeValley Community and Technical College (College).

Section 2. Scope

2.1. This Policy applies to all authorized Account Holders who have access to a College email account.

2.2. This Policy applies to shared mailboxes used by Account Holders.

Section 3. Email Usage at the College

3.1. The College will provide a College email account to all students, faculty, staff, and other Account Holders to use as an official form of communication in support of the College mission.

3.1.1. The Account Holder's email account will be created as per the guidelines established in the Account Management Policy.

3.2. As per the Account Management Policy, the contents of the College email account are the property of the College, not the Account Holder.

3.3. All employee email messages are automatically archived in compliance with the Records Retention Policy.

3.4. Although the College supports a climate of trust and respect, no Account Holder should expect complete confidentiality or privacy when using a College email account.

3.5. The College highly discourages the use of College email accounts to communicate Sensitive College Data, as outlined in the Protecting Personally Identifiable Information Policy.

3.6. If a College email account is detected to be Compromised, the Information Technology (IT) department shall promptly remedy the situation by forcing a change of the Account Holder's password.

3.7. Employees may only use their College email account to conduct College business. Personal usage that is more than de minimis (or incidental) violates this Policy and may also violate the West Virginia Ethics Act.

3.8. External Email Accounts cannot be used, in any way, to conduct College business activity.

Section 4. Shared Email Accounts and Distribution Groups

4.1. Shared mailbox College email accounts may be created for use by multiple authorized employees for a specific purpose (e.g., departmental email, committees, shared services) and must meet the following requirements:

4.1.1. Shared mailbox accounts are created for official College business use only.

4.1.2. Shared mailbox address format is departmentname@bridgevalley.edu (e.g., admissions@bridgevalley.edu) but a display name may be indicated (e.g., "BridgeValley CTC Admissions Office").

4.1.3. Shared mailbox name should be as close to the description of the department, service, or organization as possible.

4.1.4. IT department shall delegate authorized employees access to the shared mailbox. Authorized employees will access the shared mailbox using their individual email account credentials.

4.1.5. One full access delegate (owner) must be assigned to the account who is responsible for establishing formal mechanisms for granting, tracking, and terminating individual access and activity to the shared account. The owner must formally request the shared mailbox be created by written communication to the IT department.

4.2. The College may create a Distribution Group email address list to deliver email messages to a group of users.

4.2.1. The distribution group is intended to aid in communicating to a select subset of users to facilitate official College business.

4.2.2. The College's IT Department will manage groups for all employees, fulltime faculty, and all students.

4.2.3. A College employee may request for a distribution group to be created via written communication to the IT department. The user submitting the request will be listed as the owner of the group and is responsible for informing IT of the group membership additions or removals.

4.2.4. Emails sent to distribution groups can only be sent from other members within the College domain by default. IT department may restrict who can send to the distribution group internally. Also, IT may allow for external email accounts to send to the distribution group. The group owner is responsible for informing IT of the necessary delivery management requirements.

Section 5. Email Misuse at the College

5.1. Any misuse of a College email account is a violation of this Policy. Misuse includes, but is not limited to the following:

5.1.1. Using a College email account for Illegal Activities;

5.1.2. Using a College email account for activities that violate College policies;

5.1.3. Accessing another person's College email account without authorization;

5.1.4. Using an External Email Account to automatically forward/redirect a College email account to a personal email account;

5.1.5. Sending messages from a personal email account that appear to be from a College email account;

5.1.6. Sending fraudulent communications or impersonation via a College email account; and,

5.1.7. Engaging in activities that can cause direct or indirect strain on the College's computing facilities or interfere with other Account Holders' use of College email (e.g., sending spam or knowingly transmitting computer viruses).

Section 6. Email Account Holder Responsibilities

6.1. Access to the College email account is a privilege with certain accompanying responsibilities. Account Holders who use a College email account must:

6.1.1. Comply with state and federal laws, College policies, and normal standards of professional and personal courtesy and conduct;

6.1.2. Check their College email account regularly to receive College communications;

6.1.3. Exercise caution when responding to or forwarding email messages received to their College email account to avoid an inadvertent disclosure of Sensitive College Data;

6.1.4. Forward all email related to College business and received to an External Email Account to the Account Holder's College email account and notify the sender to use the College email account if future correspondence is anticipated. Marketing and other unsolicited messages may be deleted immediately without notifying the sender;

6.1.5. Never misuse a College email account; and,

6.1.6. Report any known or suspected violation of this Policy to the College IT Department.

Section 7. Definitions

7.1. Account Holders - faculty, staff, students, and other Account Holders affiliated with the College who have been assigned a college Email Account.

7.2. Compromised – an account that has been maliciously broken into and could be used by an unauthorized individual for nefarious reasons.

7.3. External Email Account – an email account not created and issued by College IT department such as AOL or Hotmail.

7.4. Sensitive College Data - data identified in the Sensitive Data Protection Policy that is subject to international, federal, or state restrictions governing its processing, storage, transmission, or use (e.g., personally identifiable information, credit card information, protected health information). If disclosed, Sensitive University Data could cause significant harm to the University or its constituents.