Baldwin Wallace University Information Technology Policy

Issued by:	**Information Technology**
Title:	**Email**
Number:	**ITP-BW-07**
Publish date:	**October 14, 2022**

1.0 Overview

Baldwin Wallace University is hereinafter referred to as "BW". BW authorized user is hereinafter referred to as “user”.

Email is an essential component of business communication; however, it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also affect BW's liability by providing a written record of communications, so having a well-thought-out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose

The purpose of this policy is to detail BW’s usage requirement for the email system. This policy will help BW reduce the risk of an email-related security incident, foster good business communications both internal and external to BW, and provide for consistent and professional application of BW’s email principles.

3.0 Scope

The scope of this policy includes BW’s email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the BW Business network.

4.0 Policies

4.1 Proper Use of BW Email Systems

Users are asked to exercise common sense when sending or receiving emails from BW accounts. Additionally, the following applies to the proper use of the BW email system.

4.1.1 Sending Email

When using a BW email account, email must be addressed and sent carefully. Users should keep in mind that BW loses any control of email once it is sent externally to the BW network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the “reply all” function or using distribution lists to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help BW avoid the unintentional disclosure of confidential or non-public information as well as reputational damage from inappropriate email content.

4.1.2 Personal Use

4.1.2.1 Current Employees or Contractors

Personal usage of BW email systems by current employees/contractors is permitted as long as such usage does not negatively impact the BW computer network, violate other parts of this policy, or the ITP-BW-01 Acceptable Use Policy. Additionally, such usage must not negatively impact the user's job performance.

> **WARNING:** Under "The Higher Education Reauthorization Act", your personal email in a BW-provided email system becomes the property of BW and may be discoverable in a lawsuit and possibly become public. Therefore, it is advised that you utilize a non-BW-provided email solution for all personal emails.

4.1.2.2 Students

Students are free to use their provided BW email account for personal use as long as the usage does not negatively impact the BW computer network, violate other parts of this policy, or the ITP-BW-01 Acceptable Use Policy.

> **WARNING:** Under "The Higher Education Reauthorization Act", your personal email in a BW-provided email system becomes the property of BW and may be discoverable in a lawsuit and possibly become public. Therefore, it is advised that you utilize a non-BW-provided email solution for all personal emails.

4.1.2.3 Emeriti

Emeriti are sometimes granted continued use of their BW email address. In such cases, emails sent to an emeritus BW email address will be automatically forwarded to an emeriti's valid personal email. The emeriti's BW email account will be disabled and deleted. The routing services provided will continue as long as such usage does not negatively impact the BW computer network, increase risk to BW, violate other parts of this policy, or violate the ITP-BW-01 Acceptable Use Policy. Emeriti are responsible to contact Human Resources for approval if this arrangement is desired.

> **WARNING:** Under "The Higher Education Reauthorization Act", your personal email routed to you via a BW-provided email system may be discoverable in a lawsuit and possibly become public. Therefore, it is advised that you utilize a non-BW-provided email solution for all personal emails.

4.1.3 Business Communications and Email

BW uses email as an important communication medium for business operations. Employees, contractors, and students on the BW email system are expected to check and respond to emails in a consistent and timely manner.

Additionally, users are asked to recognize that email sent from a BW account reflects on BW, and, as such, email must be used with professionalism and courtesy. See ITP-BW-01 Acceptable Use Policy for additional information.

4.1.4 Opening Attachments

Users must use extreme care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. BW may use methods to block what it considers to be dangerous emails or strip potentially harmful email attachments as it deems necessary.

4.1.5 Monitoring and Privacy

Users should expect no privacy when using the BW network or BW resources. Such use may include but is not limited to the transmission and storage of files, data, and messages. BW reserves the right to monitor any use of the computer network. To ensure compliance with BW policies this may include the interception and review of any emails, or other messages sent or received.

> **WARNING:** Under "The Higher Education Reauthorization Act", your email in a BW-provided email system becomes the property of BW and may be discoverable in a lawsuit and possibly become public. Therefore, think carefully before writing and sending any emails.

4.1.6 BW Ownership of Email

Users should be advised that BW owns and maintains all legal rights to its email systems, its contents, and network, and thus any email passing through these systems is owned by BW and it may be subject to use for purposes not anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that emails sent to or from certain public or governmental entities may be considered a public record.

4.1.7 Contents of Received Emails

Users must understand that BW has little control over the contents of inbound emails and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, BW may attempt to reduce the amount of this email that the users receive, however, no solution will be 100% effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email or believes that it contains illegal content, he or she must notify his or her supervisor or call the Help Desk.

4.1.8 Access to Email from Mobile Devices

Many mobile devices provide the capability to send and receive an email. This can present several security issues, particularly relating to the storage of email, which may contain sensitive data, on the device. BW permits the use of email on both BW-owned and personally owned mobile devices but requires that current employee and contractor devices have encryption enabled and requires either a PIN or biometric to access the device. See ITP-BW-05 Mobile Device Policy for additional information.

4.2 External and/or Personal Email Accounts

BW recognizes that users may have personal email accounts in addition to their BW-provided accounts. The following sections apply to non-BW provided email accounts:

4.2.1 Use for BW Business

Users must use the BW email system for all business-related emails. This includes communications between BW faculty/staff and students. Employees/contractors are prohibited from sending business emails from a non-BW-provided email account.

4.2.2 Access from BW Network

Users are permitted to access external or personal email accounts from the BW network, as long as such access uses no more than a trivial amount of BW IT resources. Users are still expected to adhere to the ITP-BW-01 Acceptable Use Policy while using a personal email from a BW network.

4.3 Confidential Data and Email

The following sections relate to confidential data and email:

4.3.1 Passwords or Passphrases

As with any BW passphrase, passphrases used to access email accounts must be kept confidential and used in adherence with ITP-BW-02 Passphrase Policy. At the discretion of the Chief Information Officer, BW may further secure email with certificates, two-factor authentication, or another security mechanism.

4.3.2 Emailing Confidential Data

Email is an insecure means of communication. Users should think of email as they would a postcard which can be intercepted and read on the way to its intended recipient.

BW requires that any email containing BW confidential information, regardless of whether the recipient is internal or external to the BW network, be encrypted using strong encryption.

Further directives on the definition and treatment of confidential information exist in ITP-BW-04 Data Classification Policy and ITS-BW-04-01 Data Classification Standard.

4.4 BW Administration of Email

BW will use its best effort to administer BW's email system in a manner that allows the users to both be productive as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email

A strategy to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe messages and removes unsolicited commercial email (e.g. SPAM). For this reason, BW may choose to filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed contrary to this policy, or a potential risk to BW's IT security. No method of email filtering is 100% effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of IT.

4.4.2 Email Retention and Deletion

Emails are considered a business record and must be retained and deleted per the applicable retention standard as defined by the ITP-BW-06 Retention Policy.

For emails not covered by a retention standard, users are encouraged to delete those emails periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable and reduce the cost burden on BW to store and backup unnecessary email messages.

Please note that users are strictly forbidden from deleting an email in an attempt to hide a violation of this or another BW policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

4.4.3 Account Termination

When a user leaves BW, or his or her email access is officially terminated for another reason, BW may disable the user's access to the account by passphrase change, disabling the account, or another method. Note, BW IT is under no obligation to block the account from receiving an email, and it may continue to forward inbound emails sent to that account to another BW email account or set up an auto-response to notify the sender that the user is no longer employed by BW.

4.4.4 Storage Limits

As part of the BW email service, email storage will be provided. The email account storage size must be limited to what is reasonable for each user, at the determination of IT. Storage limits may vary by the type of job role of the user.

4.5 Prohibited Actions

The following actions shall constitute unacceptable use of the BW email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. See ITP-BW-01 Acceptable Use Policy for additional information. Some examples, but not limited to:

- Sending any information that is illegal under applicable laws.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to BW as defined by ITP-BW-04 Data Classification Policy may not be sent via email, regardless of the recipient, without proper encryption.
- Access another user's email account:
    - Without the knowledge or permission of that user – which should only occur in extreme circumstances.
    - Without the approval of BW leadership in the case of an investigation
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene, or otherwise inappropriate messages or media.
- Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending intentionally inflammatory emails, or that include information not conducive to a professional working atmosphere.
- Make fraudulent offers for products or services.
- Attempt to impersonate another person or forge an email header.
- Send spam, solicitations, chain letters, or pyramid schemes.
- Knowingly misrepresent BW's capabilities, practices, pricing, or policies.
- Conduct non-BW-related business.

BW may take steps to report and prosecute violations of this policy, per BW standards and applicable laws.

4.5.1 Data Leakage

Data can leave the network in several ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to BW's control of its data.

Unauthorized emailing of BW data, confidential or otherwise, to external email accounts to save this data external to BW systems is prohibited. If a user needs access to information from external locations (such as from home or while traveling), that user must use approved remote access methods as defined in the ITP-BW-03 Remote Access Policy rather than emailing BW data to a personal account or otherwise

removing it from BW managed or provided systems.

BW may employ Data Loss Prevention techniques to protect against leakage of confidential data at the discretion of the IT.

4.5.2 Sending Large Emails

Email systems were not designed to transfer large files and as such emails must not contain attachments of excessive file size. BW requires the user to limit email attachments to a reasonable size as set by IT.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients and use restraint when sending large files to more than one person.

4.6 Applicability of Other Policies

This document is part of BW's cohesive set of policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

5.0 Enforcement

5.1 Employee Enforcement

This policy will be enforced by the Chief Information Security Officer, Chief Information Officer, and BW Administration. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.

5.2 Student Enforcement

Suspected misuse of the facilities should be reported to the Chief Information Security Officer (CISO) or the Chief Information Officer (CIO). The CISO and/or CIO, who is authorized to determine if there has been a violation of policy or law and refer student violators to the Office of Student Conduct for resolution. Pending the outcome, access to the shared technology resources may immediately be restricted or suspended. In some cases, limited access will be provided to the facilities needed for University-related activities, such as classes. Violations can result anywhere from Conduct Probation to suspension or expulsion from the University. Where illegal activities or theft of BW property (physical or intellectual) are suspected, BW may report such activities to the applicable authorities.