1. PURPOSE & SCOPE:

1.1 Purpose. Electronic mail (email) supports the educational, administrative, research, and outreach mission of West Virginia University (University) by serving as an official form of communication for account holders within the University community. The purpose of this Policy is to:

1.1.1 Ensure compliance with applicable laws and University policies governing email service;

1.1.2 Protect Sensitive University data;

1.1.3 Ensure the successful delivery of communications by and between the University, Faculty, Staff, and Students; and,

1.1.4 Minimize disruptions to the University email system.

1.2 Scope. This Policy applies to all authorized account holders who have access to University email accounts or are requesting authorization to use a University email system.

2. EMAIL USAGE AT THE UNIVERSITY:

2.1 The University will provide email services to all Students, Faculty, Staff, and others affiliated with it, as appropriately determined by the Chief Information Officer or their designee.

2.2 The University will use email to communicate with Faculty, Staff, and Students, and to conduct University business.
2.2.1 Account holders who are granted a University email account are expected to check it regularly to receive University communications.

2.2.2 Access to University email is a privilege with certain accompanying responsibilities. Account holders who use University-issued email accounts are required to comply with state and federal laws, University policies, and normal standards of professional and personal courtesy and conduct.

2.3 The contents of all University email accounts are the property of West Virginia University, not the account holder.

2.3.1 Although the University supports a climate of trust and respect, no account holder should expect complete confidentiality or privacy when using University email, even for personal use.

2.3.2 The University reserves the right to monitor email to ensure compliance with applicable laws and University policies. The University also reserves the right to access and review all electronic information transmitted over or stored in email and to release to third-parties when required.

2.4 The University highly discourages the use of email to communicate data classified as “Restricted” in the Data Classification Policy.

2.4.1 Approved methods of sending Restricted data electronically can be found in the ITS Restricted Data Protection Standard. To avoid an inadvertent disclosure of Restricted data, users should exercise caution when responding to or forwarding email messages.

2.4.2 Any known or suspected violation of this Policy should be reported as outlined in the Information Security Event Response Policy.

2.5 A bulk mailing service, whether supported by ITS or a third-party supplier, must be used when sending messages to more than 500 recipients.

2.6 A compromised University email account will be promptly remedied through appropriate actions outlined in the Information Security Event Response Policy.
Accounts that exhibit a repeated pattern of compromise will be suspended until the account holder has completed appropriate training.

2.7 External/personal email accounts cannot be used, in any way, to conduct WVU business activity.

2.7.1 All email received on a personal/external account that relates to University business should be forwarded to the recipient’s University-issued email account. The recipient should also notify the sender to use University email if future correspondence is anticipated. However, marketing and other unsolicited messages may be deleted immediately without notifying the sender.

2.7.2 Unacceptable use of an external/personal email account includes, but is not limited to, automatically forwarding/redirecting a University-issued email account to a personal email account, or sending messages from your personal email account that appear to be from your University-issued email account.

2.8 University email services must not be misused. Misuse includes, but is not limited to the following:

2.8.1 Using email services for illegal activities or activities that violate University policies;

2.8.2 Accessing another person’s email account without authorization;

2.8.3 Sending fraudulent communications or impersonation; and,

2.8.4 Engaging in activities that can cause direct or indirect strain on the University’s computing facilities or interfere with other account holders’ use of University email (e.g., chain letters, spam, letter bombs, knowingly transmitting computer viruses).

2.9 Faculty and Staff may only use their University email to conduct University business. Personal usage that is more than de minimis (or incidental) violates this Policy and may also violate the West Virginia Ethics Act. Account holders should abide by the guidelines set forth in the Acceptable Use of Data and Technology Resources Policy.
2.9.1 Faculty and Staff cannot use their University email to promote personal commercial activities, conduct political lobbying, or send commercial messages (e.g., advertising or sponsorship) except when the activity is clearly related to or supports the mission of the University.

2.10 Any misuse of University email services is a violation of this Policy.

2.10.1 Any Faculty or Staff who violates this Policy shall be subject to appropriate disciplinary action.

2.10.2 Any Student who violates this Policy shall be subject to appropriate disciplinary action in accordance with the Student Code of Conduct.

2.10.3 Any individual affiliated with the University who has a University email account and violates this Policy shall be subject to appropriate corrective action, including, but not limited to, cancellation of their relationship with the University.

---

3. DEFINITIONS:

3.1 **Account holder:** Faculty, Staff, Students, and other individuals affiliated with the University who have been assigned an email account that provides access to the University’s electronic mail systems.

3.2 **Compromised account:** An email account that has been maliciously broken into and could be used by an unauthorized individual for nefarious reasons.

3.3 **Email:** All electronic mail services provided, owned, or funded in part by the University and operated by West Virginia University Information Technology Services or WVU Health Sciences Center Information Technology Services. This term applies to processing, storage, transmission, and use of electronic mail data, including but not limited to email headers, summaries, and addresses associated with email records, attached files, or text. This term does not apply to voice mail, audio/video conferencing, or facsimile messages.
ITS Policy 1.1
Electronic Mail Policy

Category: Information Technology
Acceptable Use of Technology
Title: Electronic Mail Policy
Responsible Unit: Information Technology Services
Adopted: August 17, 2018
Revision History: Originally effective October 15, 2004
Review Date: August 2021

3.4 **External/personal email account:** Any email account not created and issued by West Virginia University Information Technology Services or WVU Health Sciences Center Information Technology Services.

3.5 **Illegal activities:** Illegal activities may include, but are not limited to: obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmission without proper authority; and violation of copyright, trademark, or defamation law.

3.6 **Sensitive University data:** Data identified in the Sensitive Data Protection Policy that is subject to federal or state restrictions governing its processing, storage, transmission or use, or that could cause significant harm to the University or its constituents, if disclosed. Examples include but are not limited to, personally identifiable information (PII), credit card information, protected health information (PHI), or research data.

4. **ENFORCEMENT & INTERPRETATION:**

4.1 WVU’s Chief Information Officer, supported by the Chief Information Security and Privacy Officer, will coordinate with appropriate University entities on the implementation and enforcement of this Policy.

4.2 Responsibility for interpretation of this Policy rests with the Chief Information Officer.

5. **AUTHORITY & REFERENCES:**

5.1 **West Virginia Freedom of Information Act**, W.Va code §29B-1-1 to §29B-1-7.

5.2 **West Virginia Computer Crime and Abuse Act**, W.Va code §61-3C-14a.

5.3 **West Virginia Ethics Act**, W.Va code §6B-1-1 to §6B-3-11.

5.4 **Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003**, (CAN-SPAM), Public Law No. 108-187 or 16 C.F.R Part §316.1 to §316.6.
5.5 **Stored Communications Act (SCA)**, 18 U.S.C. Chapter 121 §§ 2701–2712.

6. **CROSS REFERENCES:**

6.1 All other University policies are also applicable to the electronic environment. Relevant institutional policies and procedures include, but are not limited to:

6.1.1 [ITS Policy 1.0 - Acceptable Use of Data and Technology Resources](#)
6.1.2 [ITS Policy 2.3 – Information Security Event Response Policy](#)
6.1.3 [ITS Policy 3.2 – Sensitive Data Protection Policy](#)
6.1.4 [WVU BOG Governance Rule 1.10 – West Virginia Freedom of Information Act](#)
6.1.5 [WVU BOG Governance Rule 1.6 – Rule Regarding Discrimination, Harassment, Sexual Harassment, Sexual Misconduct, Stalking, Retaliation and Relationships](#)
6.1.6 [ITS LISTSERV Procedure](#)
6.1.7 [ITS Sensitive Data Protection Standard](#)
6.1.8 [Faculty Handbook](#)
6.1.9 [Code of Student Rights and Responsibilities (Code of Conduct)](#)
6.1.10 [WVU Culture and Talent Policies](#)
6.1.11 [WV Higher Education Policy Commission Rules and Policies](#)