

# **UNIVERSITY POLICY FOR GENERAL ADMINISTRATION**

## **Policy No. UPGA-11**

### **ELECTRONIC COMMUNICATIONS POLICY**

#### **1. General Information:**

- Authority: W. Va. Code §18B-1-6
- Passage Date: September 12, 2019
- Effective Date: October 15, 2019
- Controlling over: Faculty, Staff, Students, and Affiliates of Marshall University

#### **2. Purpose:**

- 2.1.** The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic communications. The purpose of this policy is to describe the boundaries, standards, and procedures that apply to the provision, use, regulation, administration, security and protection of the electronic communications systems in use by Marshall University.

#### **2.2. Scope:**

This policy is controlling over the provision and use of electronic communications systems within the Marshall University information technology environment

#### **2.3. Background:**

This policy was previously approved as EMAIL POLICY by the Information Technology Committee on 11/05/99 and revised 01/07/00 and Passed March 8, 2006.

### **3. Definitions:**

- 3.1.** “Affiliates” Individuals, groups, or organizations that have some relationship with the university that requires the assignment of identities, accounts, etc. from the university allowing them to use university resources.
- 3.2.** “Electronic Communications” Include forms of electronic mail (email), voice mail, “texting” (instant messaging, SMS, MMS), web and social media, forums, blogs, and web pages, etc.
- 3.3.** The Information Technology Resources (ITR): Consists of the superficial wires, equipment and devices of the data, voice, video, and more conventional information networks, processors, and storage on our campuses.
- 3.4.** Personally-Identifiable Information (PII) Refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- 3.5.** Protected Health Information (PHI): Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient’s medical record or payment history.
- 3.6.** Data Steward: A senior-level employee of the University who oversees the lifecycle of one or more sets of Institutional Data.
- 3.7.** Policy: The University recognizes electronic means of communication as official forms of communications and correspondence (some or all of which may be privileged) and, therefore, affords these electronic forms of communications all of the properties and protections comparable to that which it affords traditional forms of communications. Standards of use and conduct of electronic communications should also be extensions of current expectations, restrictions, and freedoms accorded traditional forms of communications.
- 3.8.** The University encourages the use of electronic communications and respects the privacy of users. It does not routinely inspect, monitor, or disclose electronic communications without the holder’s consent. The University may deny access to its electronic communications services and may inspect, monitor, or disclose electronic communications when it is in the best interest of the institution. The University will not attempt to regulate the content of electronic communications unless dictated by policy or law and accepts no responsibility for the content of electronic communications of individuals.

### **4. Ownership:**

- 4.1.** Marshall University is the owner of any and all content residing within or passing through the Information Technology Resources owned and operated by Marshall University where content ownership is not explicitly assigned by policy or law.

### **5. Responsibilities:**

**5.1.** The Chief Information Officer or their designee is responsible for the implementation, maintenance, and enforcement of this policy and in this role is considered the data steward of electronic communications content and systems. The implementation of this policy shall include the provision of standards and procedures that clearly define the interpretations, operational processes, maintenance, provision, regulation, and enforcement of this policy.

## **6. Eligibility:**

**6.1.** All Marshall University faculty, staff, students, departments, and affiliated persons qualify to be assigned an electronic communications account/identity that will be used for their official university correspondence. Proper verifiable identification will be required of any individual assigned an electronic communications account/identity. A detailed procedure for the assignment, maintenance, and termination of the electronic communications account/identity shall be maintained by the data steward.

## **7. Operation:**

**7.1.** Standards and Procedures insuring, in as much as is reasonably possible, the secure, reliable, effective, and efficient operation of electronic communications systems for Marshall University use will be maintained by the data steward. These include but are not limited to: backups, archiving, spam filtering, encryption, antivirus/malware filtering, copyright and intellectual property protection and leakage prevention, intrusion protection, quotas, etc.

**7.1.1.** Forwarding: Forwarding of electronic communications to systems not operated by Marshall University will be allowed but will be defined and regulated in operational procedures maintained by the data steward.

**7.1.2.** PII and PHI: Messages containing Personally Identifiable Information (PII) or Protected Health Information (PHI) are not permitted to be sent or received unless they are encrypted end to end and explicitly authorized by the President or a Vice President on a case by case basis.

Personal Use: Minimal personal use of the assigned electronic communications account is allowed as long as it in no way infringes upon or is contrary to the rights, responsibilities, mission and purpose of Marshall University, however, under no circumstances is the ITR to be used for personal gain.

## **8. Related Policies, Administrative procedures and Guidelines:**

**8.1.** MUBOG IT-1 Information Technology Acceptable Use Policy, MUBOT IT-2 Information Security Policy, MUBOG GA-14 Interim Business Record Policy

Administrative Procedures implementing this policy may be found as ITP-29 Electronic Communications Procedures on the Information Technology Council Policy and Procedures webpage. Other related Procedures include: ITG-2 Social Media Page/Account Guidelines and Tips, ITG-4 Guidelines for Data Classification ITP-4 Mass Voice Mail Distribution Procedure, ITP-5 Information Systems Identity, Access, Privilege, and Content Retention Procedure, ITP-25 Obtaining and managing a site on MU Web Server