Email & Digital Communication Policy

Purpose
ASMSA recognizes the efficiency of employing digital communications among its students and employees. Digital communication saves time, saves money, and is often the fastest, most effective method of communication among members of the ASMSA community. At the same time, digital communications can easily be abused, and an email that seems useful and pertinent to one student or employee might easily appear as "spam" to another. While email from individual to individual is sometimes troublesome, the real issue emerges about bulk or group communications, and it is this type of communication to which this policy refers explicitly.

Scope
This policy establishes standards for the electronic transmission of sensitive and business-critical data and the controls that the users will employ to protect the security and privacy of sensitive and business-critical electronic data. This policy also addresses rules and responsibilities while using ASMSA's digital communications. This policy applies to email, instant messaging, voice mail, file transfer, and any other technology that transmits sensitive and business-critical data electronically.

Definition of Terms
ASMSA Business: ASMSA business is work performed as part of an employee's job responsibilities, or work performed on behalf of the ASMSA by faculty, staff, volunteers, students, trainees, and other persons whose conduct, in the performance of work for the ASMSA, is under the direct control of the ASMSA, whether they are paid by the ASMSA.

Sensitive Data: Sensitive data is a blanket term used to designate classes of data with a high level of security that the ASMSA is legally or contractually required to protect. Sensitive data may also be referred to as protected information or personally identifiable information.

Policy
Sensitive and business-critical data that are to be transmitted electronically shall be transmitted in a manner that protects them against unauthorized access and ensures their integrity. When the circumstances allow, electronic transmission of sensitive and business-critical data, reasonable and appropriate security measures shall be implemented.

All use of email and other communication methods and tools must be consistent with ASMSA policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper business practices.

Any faculty member, staff member, or student may develop a mailing list or otherwise communicate electronically (subject to the content restrictions imposed by ASMSA's Acceptable Use Policy) with those with whom they have a supervisory, collaborative, or instructional relationship.

It is unacceptable to use the ASMSA electronic communication resources (in any form)

- To send unauthorized mass communication of any type
- To send rude, obscene, harassing, or illegal material, or material that in any way conflicts with the regulations of the ASMSA
- To send any material that in any way conflicts with state or federal law
- To send/receive individually identifiable health information, social security numbers, passwords, or any other Confidential information via the Internet or non-ASMSA email addresses
- To perform an operation or activity that degrades the performance of the ASMSA's IT systems and network
- To send E-mail with the intent of disrupting communication or other system services
- To send broadcast e-mail or listserv/group communications to users without proper institutional or divisional approval
- To intentionally distribute messages that contain viruses, worms, or other malicious code

It is extremely important that when communicating with others, including students, faculty, and staff, that users exercise extreme caution to send messages only to intended recipients. Users should only correspond with the campus community via their official @asmsa.org email address. Faculty and staff should encourage students corresponding with them via unverified personal communication methods (email, text, etc.) that they need to use their official asmsa.org email.

In general, emails sent directly from @asmsa.org to another @asmsa.org permit the sending of private and confidential information, however, extreme caution should be used. Encryption of data is highly encouraged.

- Users must recognize that email can be misdirected or forwarded on.
- Email can be stored on external devices outside of campus security controls.
- Users that routinely share confidential or protected information should never read their email via clients that could potentially store campus data on external systems.
- Users should never forward confidential or protected information to third party systems.
- Users are forbidden from using third-party email systems and storage servers to conduct ASMSA business, to create or memorialize any binding transactions, or to store or retain email on behalf of ASMSA.
- E-mail should not be the method to transmit or receive business-critical, sensitive, and personally identifiable information (PII). If transmission of PII, especially information protected by FERPA and HIPAA regulations is required, extreme caution must be

applied, and the IT Manager should be consulted before sending such transmission. It is recommended that sensitive data should be encrypted.

- Without authorization, it is forbidden to attempt to access and listen to another person's voice message, or access and read another person's e-mail, or other electronic messages or files, even when these are accidentally exposed.