Revision History

Version	Date
Email Usage Policy, 1.0	30 July 2021

EMAIL USAGE POLICY

I. Introduction

Email is an expedient communication vehicle to send messages to the USEIC community. The Organization recognizes and has established the use of email as an official means of communication. However, use of an email system at the Organization requires adequate security measures to protect the Organizational Data (as such term is defined in the USEIC Data Protection Charter (the "Charter")) that is transmitted.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy

A. Approved USEIC Email Systems

All email used to conduct Organizational business must be transmitted via an Approved USEIC Email System. For purposes of this Policy, an "Approved USEIC Email System" is Google Workspace Gmail, and any other Email System that has been risk assessed and approved by the Data Protection Officer (DPO).

B. Prohibited Actions

No User of organizational email may take any of the following actions:

- Send or forward an email through an Organizational System or Network for any purpose if such email transmission violates laws, regulations or organizational policies and procedures;
- Use any Email System other than an Approved USEIC Email System to conduct organizational business or to represent oneself or one's business on behalf of the Organization. An example of Email Systems that are not approved include a personal email account.
- Send nuisance email or other online messages such as chain letters;
- Send obscene or harassing messages;
- Send unsolicited email messages to a large number of Users unless explicitly approved by the appropriate organizational authority; or
- Impersonate any other person or group by modifying email header information to deceive recipients.

C. Provisions Relating to Emails Containing Sensitive Data

Each User shall ensure that Sensitive Data is transmitted by email only if the following conditions are met:

1. Except as provided in Section D below, all email communications of Sensitive Data are encrypted before being transmitted.
2. Sensitive Data are not transmitted in the "Subject" line of an email.

3. Before transmitting an email that contains Sensitive Data, the User verifies that no unintended information is included in the message or any attachment and that the proper document is attached.
4. Before transmitting an email that contains Sensitive Data, the User verifies the names and email addresses of the intended recipients.

D. Privacy Expectations

The Organization observes the Privacy Expectations described in the USEIC Acceptable Usage of Information Resources Policy with respect to email.

For reasons relating to compliance, security, or legal proceedings (e.g., subpoenas) or in an emergency or in exceptional circumstances, the Legal Counsel may authorize the reading, blocking or deletion of Organizational Data. In particular, in the context of a litigation or an investigation, it may be necessary to access Organizational Data with potentially relevant information. Any such action taken must be immediately reported to the Legal Counsel and the DPO.

The Organization may record information about certain data elements of email messages in the course of monitoring or maintaining its email systems. These data include but are not limited to: (a) the identity and address of the authenticated sender, (b) the address of the recipient, (c) the size of the message, (d) the transmission time, (e) the headers of the email, (f) the subject of the message, (g) the number of attachments and (h) certain features that are used to identify spam.