Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

EMAIL, SOCIAL NETWORKING, AND INTERNET USE

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of the rules and regulations regarding the use of IMSA information technology resources for email communication and use of the public Internet. It also applies to the use of IMSA technology resources for communication via social networking technologies such as Facebook and Twitter.

AUTHORIZATION

The authorization to administer, modify and enforce the provisions in this document is granted to the IMSA Chief Information Officer (CIO) by the IMSA Board of Trustees via policy **GBID Information System Technology Policy**. Therefore, this document may be changed as necessary to align with IT industry best practice without specific approval from the IMSA Board of Trustees. IMSA account holders will be notified as appropriate when changes are made.

SCOPE

This document applies to all IMSA staff, faculty and guest account holders, including but not limited to parents, alumni, board members, outside contractors and participants in outside programs. As appropriate, it also applies to participants who remotely access virtual learning environments.

EMAIL AND INTERNET USE

Electronic communication via email, social networking and general Internet access are provided primarily to advance the mission and goals Academy. However, reasonable personal use is allowed when such use does not interfere with the business of the Academy. All use of electronic communication and the Internet must be in accordance with the **Information Technology System policy GBID**.

Electronic communication (email, social networking) and Internet access through the IMSA network may not be used to:

- Solicit any commercial ventures, religious or political causes, outside organizations, or other non-IMSA related solicitations without prior approval of the IMSA Chief Information Officer, the IMSA Director of Human Resources, or their designees. However, the Academy encourages members of the IMSA community to participate in community service, and internal email messages for the purpose of supporting community service activities may be considered an IMSA-related solicitation as long as it does not conflict with any other portion of this document.

- Create, communicate, repeat or otherwise convey or receive any message or information which is offensive, illegal, indecent, obscene, defamatory, likely to cause disruption in Academy operations and programs, or is otherwise inconsistent with the Academy's curriculum and educational mission. Offensive or disruptive messages include those that contain sexual connotations, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, gender, sexual orientation, religious or political beliefs, marital status, ethnicity, national origin, military status or disability.

- Send/upload or receive/download any material or information that is offensive or disruptive, or for which the user does not have legal license.

It is required that the primary email address of any current IMSA employee be within the IMSA domain. That is, the email address for current employees must appear in the IMSA Directory as <username>@imsa.edu. Email may be forwarded to a non-imsa.edu address.

IMSA employees have access to IMSA systems and to information of a sensitive nature, including email, files, websites, etc.; access to this data may be controlled by state and federal laws. Some of these systems and the information they contain may be accessible via personal devices such as personal laptops, tablets, smartphones etc. Due to the potential for exposure of this sensitive content, IMSA staff should not download email, email attachments, files or other sensitive information to personal devices or devices regularly used offsite or operated outside of the IMSA secured network.

ENFORCEMENT

Any user of IMSA technology resources found to be in non-compliance with the provisions in this document is subject to disciplinary action under Board of Trustees policy GBDA. Such action can include one or more of the following, as appropriate: loss of the privilege of access (through suspension of system privileges or account termination), referral to law enforcement authorities, and/or disciplinary consequences, up to and including termination of employment.

EXCEPTIONS

Exceptions to this policy can be made only upon case-by-case review by the IMSA Chief Information Officer, the IMSA Director of Human Resources, or their designees.