Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

ACCEPTABLE USE

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources and of the acceptable and prohibited uses of the systems and services provided.

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 Technology System Policy**. 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 professional participants in external programs. As appropriate, it also applies to participants who remotely access virtual learning environments.

ACCEPTABLE USE OF IMSA INFORMATION TECHNOLOGY RESOURCES

Users of IMSA information technology resources must:

- Comply with all federal, state and local laws, as well as all policies, guidelines and procedures of the Academy, concerning information technology.
- Use only the information technology resources for which they are authorized.
- Use information technology resources only for their intended purpose.
- Respect the privacy and personal rights of others.
- Use secure passwords in accordance with policy **GBID Use and Enforcement of Strong Passwords**.
- Use approved Antivirus software on all computing devices connected to the IMSA production network in accordance with policy **GBID Antivirus Requirements**.

Users of IMSA information technology resources must not (but not limited to):

- Attempt to alter system software or hardware on any Academy-owned equipment without prior approval of the IMSA CIO, or designee.
- Appropriate, vandalize or otherwise abuse Academy-owned information technology resources.

- Access another individual's account, private files or email without prior permission from the owner. Access must not, in any case, violate the password requirements as stated in Use and Enforcement of Strong Passwords document.
- Misrepresent their identity in electronic communication.
- Download, install, store, distribute or facilitate the distribution of copyrighted material for which they do not have proper license.
- Initiate any network scan or denial-of-service attack.
- Use any information technology resource to access, download, upload, view or disseminate, or attempt to do so, any images or content that is obscene, pornographic, or harmful or inappropriate for students, as defined by state or federal law or determined by the IMSA President or designee.
- Use any information technology resource to threaten, harass, cyberbully, intimidate, stalk, sexually harass, or humiliate others, including but not limited to, any severe or pervasive electronic communication directed toward any IMSA community member on the basis of actual or perceived race, color, religion, sex, national origin, ancestry, age, marital status, physical or mental disability, military status, sexual orientation, gender related identity or expression, unfavorable discharge from military service, association with a person or group with one or more of the aforementioned actual or perceived characteristics, or any other distinguishing characteristic that has or can be reasonably predicted to have the effect of one or more of the following:
    - Creating a reasonable fear of harm to the individual's person or property;
    - Causing a substantially detrimental effect on an individual's physical or mental health;
    - Substantially interfering with a student or students' academic performance; or
    - Substantially interfering with an individual's ability to participate in or benefit from the services, activities, or privileges provided by IMSA.
- Use any information technology resource, Academy-owned or otherwise, for commercial or profit-making purposes or to benefit any religious or non-profit organization not affiliated with IMSA, without prior approval of the IMSA CIO, Director of Human Resources or their designees.
- Distribute unsolicited mass e-mailings of information (spam) not directly dealing with Academy business, events or announcements, without prior approval of the IMSA CIO, Director of Human Resources or their designees.
- Operate any publicly available (available from the external, public Internet) services on any information technology resources, Academy-owned or otherwise, without prior approval of the IMSA CIO, Director of Human Resources or their designees.
- Consume inappropriate amounts of bandwidth on the IMSA network. IMSA IT personnel may require the discontinuance of uses that it determines take-up inappropriate amounts of bandwidth.
- Connect any unauthorized wireless networking device to the IMSA network, or enable access to the IMSA network through a wireless device.
- Enable access to the IMSA network by unauthorized equipment through an authorized device.
- Circumvent user authentication or security of any system on the IMSA network or attempt to "hack" into any system to gain unauthorized access.
- Use IMSA information technology resources in any manner deemed to be in violation of the information in this document, or any other Academy policy or procedure.

ENFORCEMENT

All rules and procedures in this document are enforced by the IMSA CIO. 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, and the IMSA Director of Human Resources, or their designees.