Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

WARNING BANNERS AND MONITORING

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of the required use of warning banners and system monitoring.

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.

WARNING Banners and system monitoring

All Academy systems that require login must display a banner indicating the following.

- Use is for authorized persons only
- Use must be in compliance with all Federal, State and local laws and all IMSA policies
- Use may be monitored and use implies consent to be monitored
- Misuse and abuse of systems may be reported to law enforcement or other appropriate officials

Current banner

"This system is for the use of authorized persons only. All use must be in accordance with Federal, State and local laws and all IMSA policies. Individuals using this computer system without authority, or in excess of their authority, are subject to having their activities on this system monitored and recorded by appropriate personnel. In the course of normal system administration, or while monitoring suspected unauthorized use, the activities of authorized users may also be unintentionally monitored. By continuing to use this system, all users expressly consent to this monitoring and are advised that if such monitoring reveals possible criminal activity or violation of IMSA policy, evidence of such activity may be provided to law enforcement or other officials."

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.