Illinois Mathematics and Science Academy®

INFORMATION TECHNOLOGY SYSTEM

WIRELESS COMMUNICATIONS AND NON-STUDENT PERSONAL WIRELESS DEVICES

PLEASE NOTE: this document will not be in effective until 10/1/2014. Until then, personal wireless devices are permitted only by explicit permission of the IMSA CIO for purposes of beta testing.

PURPOSE

The purpose of this Information Technology System document is to inform all users of IMSA technology resources of the requirements for the use of wireless devices, Academy-owned or otherwise, on the IMSA campus.

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 professional participants in external programs. As appropriate, it also applies to participants who remotely access virtual learning environments. It applies to any device with wireless capabilities, including, but not limited to, computers, laptop computers, tablets and phones.

WIRELESS COMMUNICATIONS AND PERSONAL WIRELESS DEVICES

IMSA offers wireless network access via both secure and non-secure connections. The enterprise network is only accessible via secure connections, and is available only to those users with IMSA accounts. Access to the public Internet, and a limited subset of internal websites, is available via open, non-secure wireless networks.

Personal wireless devices (smartphones, tablets, laptops, etc.) may not be used on the IMSA enterprise wireless network unless such use is needed to fulfill job requirements. Approval from the employee's supervisor is required. Personal wireless devices may be used on the non-secure "guest" wireless networks without approval, where and when available, provided such use does not interfere with the business of the Academy.

In order to use an approved personal wireless device on the IMSA network, users must agree to the terms and conditions outlined in this document. Connection to the IMSA network, its data and applications, implies acceptance of these terms and conditions.

- Wireless access points (routers) other than those configured and operated by ITS are not allowed to be connected to the IMSA network
- Wireless devices other than those configured and operated by ITS cannot be connected to any other device connected to the IMSA network.
- Users must be granted explicit permission by ITS to access the secure internal IMSA wireless network.
- 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.
- Upon connecting an approved personal wireless device to the IMSA wireless network, certain features, including but not limited to, access to local storage, access to Bluetooth, access to a local camera or voice recording functions, may be unavailable.
- When connected to the IMSA collaboration suite (Zimbra) with a personal wireless device, certain features, including but not limited to, access to local storage, access to Bluetooth, access to a local camera or voice recording functions, may be unavailable.
- In the event that a personal wireless device is lost or stolen, IMSA ITS reserves the right to remotely access and wipe (erase) data up to and including the complete contents of the device memory and configuration, as needed to protect sensitive IMSA data.

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, the IMSA Director of Human Resources, or their designees.