ILLINOIS MATHEMATICS AND SCIENCE ACADEMY®

SECTION G - PERSONNEL

INFORMATION TECHNOLOGY SYSTEM POLICY

PURPOSE

The purpose of the Illinois Mathematics and Science Academy (IMSA) Information Technology System (ITS) Policy is to create an environment that maintains the confidentiality, integrity and availability of information technology resources and data at IMSA. Inappropriate use of information technology resources exposes IMSA to risks that can compromise those resources (including, but not limited to: network systems, servers, devices, services) and ultimately, data and information vital to fulfilling the mission and goals of IMSA.

This policy also exists to inform the users of the IMSA computing system of their obligations for protecting technology resources and Academy data.

AUTHORIZATION

The Board of Trustees of IMSA hereby authorizes the Chief Information Officer of IMSA to update the procedural documents referenced in this policy, annually as appropriate and/or required, in compliance with industry best practices and as reasonable and practicable at IMSA.

SCOPE

This policy applies to all IMSA staff, faculty, alumni and guests (e.g., parents, board members, external contractors, etc.) who access and use information technology resources. As appropriate, it also applies to participants who remotely access virtual learning environments.

It addresses:

- Privacy
- General policy concerning secure use of the IMSA computing system
- Acceptable use of information technology resources
- Requirements for strong passwords
- Electronic communication and Internet use
- Warning banners and monitoring
- Antivirus requirements

- Security Awareness
- Wireless communications
- Remote access
- Account retention
- Use of external web sites

It is not the intention of this policy to detail all issues and system specifics. Separate procedures, standards and guideline documents, viewable on the IMSA main website, provide issue specific and system specific details. These external documents are authoritative and binding.

PRIVACY

IMSA desires to provide a secure computing system for users. However, users of IMSA computing and networking resources may not assume an expectation of privacy of data created, transmitted or stored on Academy-owned systems. Information technology resources are subject to monitoring and audit by authorized IMSA personnel. Data gathered in such an audit may be provided to law enforcement or other officials or used in disciplinary proceedings.

In their use of IMSA information technology resources, IMSA employees shall maintain the confidentiality of student records and information.

GENERAL POLICY

Use of the information technology resources of the Illinois Mathematics and Science Academy is a privilege. IMSA's information technology resources, and the data contained therein, must only be used in a manner that will preserve and protect their confidentiality, integrity and availability. Failure of users to utilize the resources in accordance with this policy or any administrative procedures, or misuse of the resources, will result one or more of the following: loss of the privilege of access, referral to law enforcement authorities, and/or disciplinary consequences, up to and including termination of employment.

Although it is recognized that there should be free and open access to information, (see policy IBA, Freedom of Access to Information and Educational Resources), information technology resources and IMSA data must be protected to ensure the fulfillment of the Academy's mission and goals.

IMSA reserves the right to block or filter Internet access to technology resources, including the public Internet, when such access is counter to the mission and goals of the Academy, or is otherwise required by law. Filtering devices shall protect against Internet access by adults or students to visual depictions or content that is obscene, pornographic, or harmful or inappropriate for students as defined by state or federal law,

or as determined by the IMSA Chief Information Officer, the IMSA Vice President of Human Resources, or their designees. The IMSA Chief Information Officer, the IMSA Vice President of Human Resources, or their designees, shall enforce the use of filtering devices and IMSA procedures regarding the use of information technology shall address the following:

- Ensure staff supervision of student access to online electronic networks;
- Restrict access to inappropriate or harmful material;
- Ensure student and staff privacy, safety, and security when using electronic communications;
- Restrict unauthorized disclosure, use, and dissemination of personal identification information, such as names and addresses; and
- Restrict unauthorized access, "hacking," or other unlawful activities.

If authorized by the IMSA Chief Information Officer, the IMSA Vice President of Human Resources, or their designees, filtering devices may be disabled for bona fide research or other lawful purposes.

By using IMSA information technology resources, account holders agree to accept and abide by all terms and conditions contained in IMSA IT policies, procedures, standards and guidelines.

ACCEPTABLE USE OF 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
- 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

Details concerning acceptable and prohibited use can be viewed in the **Acceptable Use Procedures** Document on the IMSA website.

USE AND ENFORCEMENT OF STRONG PASSWORDS

- All IMSA accounts must use strong passwords in accordance with current IT best practices.
- All IMSA systems requiring login can only be accessed via encrypted connections in accordance with current IT best practices.

Details concerning password strength and requirements can be viewed in the **Use and Enforcement of Strong Passwords** Document on the IMSA website.

ELECTRONIC MAIL AND INTERNET USE

Email, access to social networking sites and 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 and otherwise complies with acceptable use procedures.

Details concerning Email and Internet use can be viewed in the **Email, Social Networking and Internet Use** document on the IMSA website.

WARNING BANNERS

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

Details concerning banners and monitoring can be viewed in the **Warning Banners and Monitoring** document on the IMSA website.

ANTIVIRUS REQUIREMENTS

All devices including, but not limited to desktop, laptop and tablet computers connected to the IMSA network are required to have installed software designed to detect and eliminate malware, including viruses, worms and Trojan horses. Any computer determined to be infected with and/or spreading malware will be disconnected from the IMSA network.

Details concerning antivirus requirements can be viewed in the **Antivirus Requirements** document on the IMSA website.

SECURITY AWARENESS

All IMSA employees are required to attend a presentation covering security awareness, as it relates to the use of IT resources, before they receive access to their assigned account. This is part of the employee on-boarding process. In addition, all employees may be required to take periodic refresher training.

Details concerning security awareness training can be viewed in the **Security Awareness** document on the IMSA website.

WIRELESS COMMUNICATIONS AND PERSONAL WIRELESS DEVICES

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

Details concerning wireless communications and use of personal devices can be viewed in the **Wireless Communications and Personal Wireless Devices** document on the IMSA website.

REMOTE ACCESS

Remote access to IMSA technology resources through Virtual Private Network (VPN) connections enables offsite users to operate as if they were connected to the network on-campus. Secure VPN connections are provided to those users with IMSA accounts, and whose work requires or allows access from offsite.

Details concerning wireless communications and use of personal devices can be viewed in the **Remote Access Procedures** document on the IMSA website.

ACCOUNT RETENTION

IMSA staff, faculty and external users are not allowed to retain their IMSA accounts after leaving IMSA (retirement, resignation, dismissal, sunset date, etc.). However, former employees who leave in good standing may be allowed to request a forwarding address for email sent to their IMSA account name. An exception is made for those former employees who have been granted emeritus status.

Details concerning account retention can be viewed in the **Account Retention** document on the IMSA website.

USE OF EXTERNAL SITES

The use of external web sites, social networking sites or video sites to communicate, advertise, promote or otherwise display official IMSA business is permitted, provided that content is approved prior to publishing by IMSA Marketing and Communications. Branding of this external content may also be required prior to publishing.

Details concerning the use of external sites can be viewed in the **External Sites** document on the IMSA website.

POLICY ENFORCEMENT

This policy is enforced by IMSA Human Resources. Any user of IMSA technology resources found to be in non-compliance with this policy or any administrative procedure is subject to disciplinary action under policy GBDA. Such action may 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 Vice President of Human Resources, or their designees.

ADOPTED: September 10, 2002
AMENDED: November 16, 2005
AMENDED: May 18, 2011
AMENDED: May 16, 2014