Policy JBID

ILLINOIS MATHEMATICS AND SCIENCE ACADEMY

SECTION J - STUDENTS

INFORMATION TECHNOLOGY SYSTEM POLICY

I.   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 (network systems, servers, 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.

II.   SCOPE

This policy applies to all users of IMSA information technology resources, including students and alumni accessing information technology resources. It addresses

- General policy concerning secure use of the IMSA computing system
- Acceptable use of information technology resources
- Requirements for strong passwords
- Email and Internet use
- Warning banners
- Antivirus requirements
- Wireless communications
- Account retention

It is not within the scope of this policy to detail all of the system-specific uses of IMSA information technology resources. Separate standards and guidelines cover these issues and can be reviewed on the IMSA website .

III.   PRIVACY

IMSA desires to provide an assured level of confidentiality to users of the computing system. 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. When there is reasonable belief that local, state or federal laws, or IMSA policies have been violated, 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.

IV.   DEFINITIONS

Information technology resources
   Any computer, networking device, telephone, copier, printer, fax machine or other information technology which is owned, licensed or leased by IMSA is subject to IMSA policies. In addition, any information technology which (1) connects directly to the IMSA data or telephone network, (2) connects directly to a computer or other device owned or operated by IMSA, or (3) otherwise uses or affects IMSA information technology resources is subject to IMSA information technology policies, no matter who owns it.

Users
   Two broad classes of users exist.
   - <u>Regular users</u> (students and parents of current students) are entitled to use all or most IMSA technology and services.
   - <u>Special users</u> (alumni) are entitled to use specific, limited services for specific purposes under specific conditions.

Confidentiality, integrity and availability
   Assurance that data is protected from unauthorized access, has not been altered in storage or transmission and is accessible by authorized personnel on demand.

ITS
   Information Technology Services

Malware
   Malicious software— software code that is developed with the intention to cause harm or which is actually used to cause harm.

Services
   Processes on a computer system that provide access to remote users, e.g. web server or email server.

Publicly available
Implies access is available to the general public (non-IMSA community) via the Internet

V. 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 intentional 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 suspension or dismissal from educational programs.

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 when such access is counter to the mission and goals or academic standards of the Academy. The IMSA computing system is operated in accordance with Information Technology best practices such as those documented in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2196 (Site Security Handbook).

VI. ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Acceptable Use

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 Section VII.
- Use approved Antivirus software on all computers in accordance with Section X.

Prohibited Use

Users of IMSA information technology resources must not:
- Attempt to alter system software or hardware on any Academy-owned equipment without prior approval of the IMSA Executive Director of Information Technology Services (EDITS) 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 given in Section VII.
- 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 threaten, harass, intimidate, stalk, sexually harass, or humiliate others, including but not limited to, any severe or pervasive electronic communication directed toward a student or staff 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:
  o Placing the student or students in reasonable fear of harm to the student's or students' person or property;
  o Causing a substantially detrimental effect on the student's or students' physical or mental health;
  o Substantially interfering with the student's or students' academic performance; or
  o Substantially interfering with the student's or students' 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 IMSA senior administration.
- Distribute unsolicited mass e-mailings of information (spam) not directly dealing with Academy business, events or announcements, without prior approval of the IMSA EDITS or designee. (For more information, see the Mass Email Guideline on the IMSA web.)
- Operate any publicly available services on any information technology resources, Academy-owned or otherwise, without prior approval of the IMSA EDITS or designee.
- Consume inappropriate amounts of bandwidth on the IMSA network. IMSA 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.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.

VII. USE AND ENFORCEMENT OF STRONG PASSWORDS

Passwords are an important aspect of computer and network security. They are the front line of protection from network intrusion, protection of user accounts, and ultimately, protection of IMSA's data. A poorly chosen and maintained password can compromise the integrity of IMSA's entire system.

The password requirements below apply to all IMSA community members who have or are responsible for an account (or any form of access that supports or requires a password) on any system operated by IMSA ITS. These requirements also apply to any system that has access to the IMSA network, or stores any non-public IMSA information, regardless of its location.

Password Requirements

- All passwords must be changed on a regular basis in accordance with State of Illinois guidelines and IMSA ITS standards.Passwords must not be communicated via email.
- Passwords must be a minimum of eight (8) characters long.
- Passwords must be a mixture of upper and lower case letters, numbers and special characters (!@#$%^&*, etc.).
- Passwords may not be reused within a cycle of six changes.
- Passwords must not be a word that appears in any dictionary in any language, forwards or backwards, or any word of slang or jargon.
- Passwords must not be shared between users, at any time, in any circumstance.
- Passwords must never be communicated to anyone claiming to need them for purposes of verification of identity.
- Passwords must not be written down and stored in insecure locations.

Password Testing

Designated IMSA IT personnel will regularly test passwords, using readily available password testing tools. If a password does not meet the strong password requirements outlined above and can be "cracked," the account will be locked.

VIII. ELECTRONIC MAIL AND INTERNET USE

Electronic mail (email) and Internet access are important to all users of the Information Technology system to help the Academy fulfill its mission and goals.

All use of email and the Internet must be in accordance with other portions of this policy.

IMSA email and Internet access through the IMSA network may not be used to:

- Solicitation of any commercial ventures, religious or political causes, outside organizations, or other non-IMSA related solicitations is prohibited. 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 policy.

- 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.

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

IX.   WARNING BANNERS

All Academy-owned systems that allow valid IMSA account holders to log in to internal systems must display the following 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."

X.   ANTIVIRUS REQUIREMENTS

All computers connecting 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.

XI. WIRELESS COMMUNICATIONS

IMSA provides access to internal services and the Internet via secured wireless network connections for those users that have been pre-approved for this access. Direct access to IMSA networks via unsecured wireless communication mechanisms is prohibited. Only wireless systems that meet the criteria of this policy or have been granted an exception by the IMSA EDITS or designee are approved to connect to IMSA's networks.

This standard applies to all wireless data communication devices including, but not limited to, wireless access points, personal computers and PDAs connected to any of IMSA's internal networks. Wireless access via devices which do not connect directly to IMSA's network is not covered. Cellular phones are specifically excluded.

- Wireless access points 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.

- In all cases, users must be granted explicit permission by ITS to access the IMSA internal wireless network.

XII. ACCOUNT RETENTION

Students and Alumni

IMSA wishes to encourage continued contact with and involvement of former students, and may facilitate that involvement with active accounts. Alumni may continue to be granted access privileges on IMSA technology resources for an indefinite period of time, irrespective of accounts or access they may have on other systems.. All former students who have not graduated shall be permitted accounts on the same basis as graduated students if they were allowed to maintain their account at the time they left the Academy. Accounts that are inactive for a period of one year may be terminated.

XIII. REMOTE ACCESS TO IMSANET

Remote access to the IMSA network through Virtual Private Network (VPN) or dial-up connections enables users to operate as if they were connected to the network on-campus. Remote users are subject to the provisions of this and all sections of this policy.

Remote access has been instituted to advance the work of the Academy. It is an enhancement to the established network services, offering an alternative method of entry for those who must perform all or some of their work from off-campus.

It is the responsibility of IMSA students and alumni with remote access privileges to the IMSA network to ensure that their remote access connection is given the same consideration as the user's on-site connection at IMSA.

The remote user bears responsibility for the consequences if the access is misused.

All computers that are connected to IMSA's network via remote access must use Antivirus software in accordance with Section X of this document.

Remote access is available to:
- Current students. Remote access may be useful to students when they are off-campus. Access will be considered on a case-by-case basis and may be provided under the following circumstances:
  o The student is currently enrolled and has an active network account.
  o The need for access is requested during the academic calendar year.
  o The student is located off-campus.
  o Student access will be granted for a specified time period agreed upon and stated in advance of approval. At the end of this time, access will be terminated.
- All other valid account holders may be granted remote access on a case-by-case basis. Access will only be granted to those who have specific IMSA responsibilities which advance the mission and work of the Academy and for which other access means are not available or practical.

XIV. ENFORCEMENT

Any user of IMSA technology resources found to be in non-compliance with this policy is subject to disciplinary action under Policy JG – Student Discipline.

XV. EXCEPTIONS

Exceptions to this policy can be made only upon case-by-case review by both the IMSA EDITS and Director of Student Life or their designees.