ABUDHABI INDIAN SCHOOL IT POLICY

Name of Policy	:	IT Policy
Purpose of the policy	:	To provide the guideline for the usage of IT facilities and resources in Abu Dhabi Indian School
Approval for this Policy given by	:	Hon. Chairman, B.O.G
Responsibility for its update	:	Chairman, BOG
Policy applies to	:	To all staff and students of Abu Dhabi Indian School
Date of Approval	:	01-07-2014 (Amended in April 2017)
Proposed Date of Review	:	01-07-2019

ABUDHABI INDIAN SCHOOL IT POLICY

INTRODUCTION

Abu Dhabi Indian School maintains certain policies with regard to the use and security of its computer systems, networks, and information resources. All users of these facilities, including technology developers, end users, and resource administrators, are expected to be familiar with these policies and the consequences of violation.

Information technology policies ensure that everyone's use of the school's computing and telecommunications resources supports its educational, research, and administrative mission in the best possible way.

Information Technology Resources policy for the school provides for access to information technology (IT) resources and communications networks within a culture of openness, trust, and integrity. In addition, ADIS is committed to protecting itself and its students, faculty, and staff from unethical, illegal, or damaging actions by individuals using these systems.

PURPOSE

The purpose of this policy is to outline the ethical and acceptable use of information systems at Abu Dhabi Indian School. These rules are in place to protect students, faculty, and staff; i.e., to ensure that members ADIS have access to reliable, robust IT resources that are safe from unauthorized or malicious use.

Insecure practices and malicious acts expose ADIS and individual students, faculty, and staff to risks including virus attacks, compromise of network systems and services, and loss of data or confidential information. Security breaches could result in legal action for individuals or the school. In addition, security breaches damage the school's reputation and could result in loss of services. Other misuses, such as excessive use by an individual, can substantially diminish resources available for other users.

SCOPE

The IT security policy applies to faculty, staff, and students as well as any other individuals or entities who use information and IT resources at Abu Dhabi Indian School. This policy applies to all IT resources owned or leased by ADIS and to any privately owned equipment connected to the campus network and includes, but is not limited to, computer equipment, software, operating systems, storage media, the campus network, and the Internet.

Securing and protecting these significant and costly resources from misuse or malicious activity is the responsibility of those who manage systems as well as those who use them. Effective security is a team effort involving the participation and support of every member of the ADIS community who accesses and uses IT resources. Therefore, every user of ADIS's IT resources is required to know the policies and to conduct their activities within the scope of the policy. Failure to comply with this policy may result in loss of computing privileges and/or disciplinary action.

POLICY STATEMENT

The use of information technology resources in Abu Dhabi Indian School is restricted to purposes related to the school's mission. Eligible individuals are provided access in order to support their studies, instruction, duties as employees, official business with the school, and other school-sanctioned activities. Individuals may not share with or transfer to others their school accounts including network IDs, passwords, or other access codes that allow them to gain access to school information technology resources.

UNACCEPTABLE USE

Users are prohibited from engaging in any activity that is illegal under law or in violation of school policy. The categories and lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

➢ Excessive Non-Priority Use of Computing Resources

Priority for the use of IT resources is given to activities related to the school's missions of teaching, learning, research, and outreach. School computer and network resources are limited in capacity and are in high demand. To conserve IT resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of IT resources, such as recreational activities and non-academic, non-business services.

➢ Unacceptable System and Network Activities

Unacceptable system and network activities include:

- Engaging in or effecting security breaches or malicious use of network communication including, but not limited to:
    - Obtaining configuration information about a network or system for which the user does not have administrative responsibility.
    - Engaging in activities intended to hide the user's identity, to purposefully increase network traffic, or other activities that purposefully endanger or create nuisance traffic for the network or systems attached to the network.
    - Circumventing user authentication or accessing data, accounts, or systems that the user is not expressly authorized to access.

➢ Unauthorized Use of Intellectual Property

Users may not use school facilities or networks to violate the ethical and legal rights of any person or company protected by copyright, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

- Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publication of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; copyrighted music or video; and the installation of any copyrighted software without an appropriate license.

- Using, displaying, or publishing licensed trademarks without license or authorization or using them in a manner inconsistent with the terms of authorization.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.

➢ Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

- Setting up file sharing in which protected intellectual property is illegally shared.
- Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Inappropriate use or sharing of school-authorized IT privileges or resources.

- Changing another user's password, access, or authorizations.
- Using an ADIS computing asset to actively engage in displaying, procuring, or transmitting material that is in violation of sexual harassment policy or laws, hostile workplace laws, or other illegal activity.
- Using an ADIS computing asset for any private purpose or for personal gain.

➢ Misuse of Electronic Communications

Electronic communications are essential in carrying out the activities of the school and to individual communication among faculty, staff, students, and their correspondents. Individuals are required to know and comply with the school's policy on mass email and effective electronic communication**.**

Key **prohibitions** include:

- Sending unsolicited messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material, except as approved under the IT policy.
- Engaging in harassment via electronic communications whether through language, frequency, or size of messages.

- Masquerading as someone else by using their email or internet address or electronic signature.
- Soliciting email from any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or solicitations for business schemes.
- Using email originating from ADIS provided accounts for commercial use or personal gain.

USER ACCOUNTS & PASSWORDS

All ADIS User Accounts will be protected by effective passwords. An effective password is both strong and protected. Strong passwords have at least a specified minimum number of characters, are a combination of alphabetic, numeric and special characters, and are not common dictionary words. Account holders and system administrators, acting as account/password custodians, will protect the security of those passwords by managing passwords in a responsible fashion.

Anyone who has an official affiliation with ADIS may require access to school's computer services in order to perform work for the school and so should receive an account.

The formation of an account creates a unique, non-transferable electronic identity to each staff member. Account holders are immediately authorized to send/receive email using an "@adisuae.com" address, are provisioned with standard email quota, may begin to create and share files, are provisioned with standard shared file storage quota, and are otherwise entitled to use or participate in all facilities, services, and resources offered by school that are generally available to ADIS accounts and do not require additional authorizations.

Length of Time for Accounts. Regular Accounts remain in effect throughout the individual's official affiliation with ADIS. When an individual's affiliation ends or changes status, school has a standing process for deactivating accounts that no longer meet ADIS's eligibility requirements. The timing of the deactivation depends on the nature of the prior affiliation with ADIS and the circumstances of its ending. For example, accounts of staff who resigns will be deactivated once the service period ends.

- **Rationale**

  Account holders are held responsible for all activities associated with their accounts. As such, the strength and protection of the password is critical to ensuring that unauthorized activity does not become associated with a person's account. Each computer user is responsible for his or her use of technology on campus. The integrity and secrecy of an individual's password is a key element of that responsibility.

- **Implementation**

  Account holders should:

  - Create a strong password.

- Change the password as frequently as needed to ensure security for the resources computers, data, etc. under their control
- Safeguard their password. For example, individuals should not write down or store the password on paper or on a computer system where others might acquire it.
- Never share their password, even with a best friend or relative. We recognize there may be times when people need to have someone do something on their behalf, when work is being delegated, and lack of access to an account might impede business. That said, we want to emphasize that when you give someone your password, they may take actions in your name that you might not be aware of, might not approve of, but may be held responsible for depending on the nature of the activity.
- Never reuse their user name and password for external services, be they related to school business or of a personal nature.
- Change their password immediately if they know or suspect that it has been guessed, stolen, intercepted, or otherwise compromised. Contact the IT Department of the school for further guidance and assistance if this occurs.

System administrators and service provides are expected to:

- Store account passwords such that they cannot be produced on demand under any circumstances.
- Prevent, or take steps to reduce the likelihood of, the exposure of any clear text account passwords that an ADIS application, system, or other service has received for purposes of authentication.
- Never request that passwords be sent over the Internet in the clear. Of particular importance is that passwords never be sent via email.

IT STAFF ACCESS TO CONFIDENTIAL DATA

IT staff accessing or disclosing private or sensitive information within ADIS enterprise systems that is outside the specific job responsibilities is prohibited without the approval of the school authorities.

IT staff provide systems and application administration for servers under their management. In order to perform these activities and provide support for these systems, IT staff may have administrative access to the operating system, databases, or applications being supported as part of their job responsibilities. This access may only be used in support of school and consistent with the roles and responsibilities of the staff member as prescribed by ADIS management. IT staff periodically reviews administrator access to the systems it is responsible for managing, and administrative access is also reviewed and updated upon a change in the staff member's role or responsibilities.

ACCESS TO COMPUTING RESOURCES

ADIS's campus-wide computer network, connects many workstations, printers, and servers. But connectivity also requires that users of the network understand their responsibilities in order to protect the integrity of the system and the privacy of other users.

- Don't violate the intended use of the ADIS system.
  - Don't use ADIS resources for non-educational purposes in any way that interferes with their use for educational purposes.
  - Don't use any software available on ADIS for any non-educational purpose if the license for that software does not permit such use. In many cases, software available on ADIS is licensed for educational use only.
  - Access to the computing facilities is restricted to authorized members of the ADIS community.
  - Don't reconfigure the cluster, either hardware or software.
    - Moving equipment will often cause damage, or may cause it to be reported as stolen. Permanent damage may result from even unplugging a keyboard.
    - Similarly, altering a workstation's file system in any way may render the machine unusable, or threaten its usability in other ways. For example, you should not reconfigure any workstation in ADIS cluster to allow remote connections unless you are actually sitting at that workstation. Even an apparently "harmless" change such as this (i.e., changing the access configuration of a workstation) may create major system security problems.
    - Also, do not remove any equipment -- or furniture!
    - If you believe the configuration of a cluster needs to be changed, you can contact the school IT Department.

SOFTWARE ASSET MANAGEMENT

- It is the policy of the Abu Dhabi Indian School to respect all software copyrights and license agreement terms/conditions that apply to the school owned software installed on its IT facilities.
- Users may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless expressly authorized to do so under the prevailing software agreement.
- Users may not give licensed or copyrighted software to any external parties, including, but not limited to clients, contractors, customers, unless expressly authorized to do so under the prevailing software agreement.
- Users may use software on local area networks, licensing servers, or on multiple machines only in accordance with the prevailing software agreement.

- Assistance with software copyright or license arrangements can be obtained from the school’s IT Department.

ACQUISITION OF SOFTWARE

- To purchase software, users should obtain approval from school management.
- Once the software has been received and installed, the IT Department is responsible for ensuring that the original media, license documents, manuals and other associated material are securely kept and appropriately stored as school managed asset.

INSTALLATION & REMOVAL OF SOFTWARES

The IT Staff of the school is responsible for ensuring only authorized and trained staff install and uninstall the software on the school IT facilities. The IT Department should be able to produce the original media, license documents, manuals and other associated material as required, for formal audits or license checks.

INTERNAL AUDIT

The IT Department should conduct half-yearly audits for software assets under their control. This activity will be completed on a random basis and will affect desktops, laptops and servers. The audit will identify all software assets installed on randomly selected IT facilities and will test to ensure compliance with all relevant software licensing terms and conditions. All staff should cooperate with IT team when conducting these audits.

HARDWARE ASSET MANAGEMENT

School has provided hardware resources for the use of Staff and students like desktops, laptops, printers, Smart Boards, Projectors, Tablets, Biometric machines etc. All users must follow the IT policy and they must behave appropriately and use them in an acceptable manner for them to be allowed at Abu Dhabi Indian School.

INTERNET ACCESS

Access to the internet from ADIS must be in support of educational research or learning:

- Accessing any newsgroups, list services, web pages or other areas of cyberspace that would be considered offensive or which can be perceived as dangerous, anti-social, rude or inappropriate is strictly forbidden.
- Non-educational games or “chat’’ lines are not permitted.

- Email must not be sent to “all users”.
- Plagiarism is unacceptable. Therefore, all material downloaded for assignments must be formally acknowledged in an appropriate manner listing its source in a bibliography and clearly specifying any directly quoted material.

ADDITIONAL RESPONSIBILITIES

In consideration of the privilege of accessing and using the IT Resources, all Users must fully comply with the standards and responsibilities of acceptable use as outlined in:

- This IT Policy in its entirety including the related policies: Anti-Spam Policy, Email Policy, Peer-to-Peer Policy, Hosting Policy, Wireless Policy, and Internet Usage Policy;
- All software license agreements acquired by the school and its authorized units;
- Software must not be copied except with the express permission of the copyright holder.
- Software must not be adapted (including translation from one language to another) without the express permission of the copyright holder.
- The School computer facilities must not be used to make illegal copies of any piece of software.
- Illegally obtained software must not be used on the School computer facilities.
