INDIAN SCHOOL RAS AL KHAIMAH, UAE

SCHOOL POLICIES –

IT POLICY 2022-23

DECEMBER 2018
REVIEW AUGUST 1,2020
NEXT REVIEW: MARCH 2021
REVIEWED ON MAY 2022
NEXT REVIEW: MAY 2023

POLICY STATEMENT

IT Policy created and mandatory to implement for maintaining, securing and ensuring the legal and appropriate use of IT resources of Indian School Ras Al Khaimah. The policy terms assure a school community with a high-quality, trusted and secure computing environment, with a responsibility to protect and secure its property interests, data, and intellectual property. Furthermore, the School requires people to use its information technology resources responsibly, abiding by applicable laws, policies, and regulations.

REASON FOR POLICY

The School provides information technology resources to a large and diverse group, including faculty, staff, students, and visitors. All members of this community are responsible for using these resources ethically and respectfully that protects them and follows the IT policies.

SCOPE

This policy applies to everyone who uses School IT resources, whether physically located on the school campus or remotely connected. Hence this policy applies to all electronic information stored or transmitted on the School Network and the supporting IT infrastructure and covers all students, teachers, and staff – whosoever uses the School network, and IT device belongs to School. All members of the School community should read this policy.

INTRODUCTION

All staff and students are provided access to the School computer network and the Internet. The policy on the IT infrastructure aims to regulate its use by all its authenticated users and respectable guests. Thus everyone uses it appropriately and lawfully for the continuous availability of network and Internet access.

- It is the policy of Indian School Ras Al Khaimah to ensure that:
- The whole IT resource has been appropriately managed.
- information will be protected against unauthorized access
- confidentiality of data will be assured
- the integrity of data will be maintained
- regulatory and legislative requirements will be met
- business continuity plans will be produced, maintained and tested
- training related to IT resources access will be available to all staff

When implemented and followed, the policy ensures that the electronic information is provided to maintain its mission of education, research, and service.

ROLES AND RESPONSIBILITIES

Everyone agrees to abide by the policy terms by accepting account access and related information and accessing School devices, networks or Internet systems.

The following are significant responsibilities each party has in connection with this policy:

- The governing body has the ultimate corporate responsibility for ensuring that the School complies with the legislative requirements relating to the use of IT systems and for disseminating policy on IT security and other IT-related matters.
- The Principal is responsible for ensuring that the legislative requirements relating to the use of IT systems and networks are met and that the School's IT Policy, as may be amended from time to time, is adopted and maintained by the School.
- IT Department: Implement operational, physical, and technical controls for access, use, transmission, and disposal of data compliance with all privacy and security policies, procedures, and guidelines. The day to day functions is delegated to the IT admin.
- User: Use all (IT) resources and data in a legal, ethical, and consistent manner with the mission of education and research.

TERM OF PERMITTED USE

"The School has the right to suspend the access to its IT resources and related services for technical reasons, policy violations, or other concerns."

Internet facility can be accessed by the teachers and staff members using lan / wifi connectivity. It is expected that teachers/Staff members use a cabled network as the preferred network. If teachers/staff members are bringing their own devices, they can connect through wifi, where BYOD policy and all other related policies should be followed strictly.

Internet access can be granted to visitors on demand of concerned faculty/staff members.

School offers access to its network and Internet facility for educational and research purposes only. If one is unsure of the business activity, use whether appropriate or not, one must consult the IT admin staff for usage.

GENERAL RULES

All users must comply with Rules, Regulations and Policies, cyber laws and the terms of (applicable) contracts, including software licenses, while using School IT resources. It may include but is not limited to: privacy, copyright, trademark, obscenity and child pornography, hacking, cracking and similar activities, Scams etc.

Users are responsible for ascertaining the necessary authorizations before using the School IT resources. In addition, they are responsible for the activities from their accounts. Under any circumstances, Accounts and passwords must not be used by persons other than those the account administrator has assigned them. Any detection/suspect of unauthorized use of accounts or resources must be reported to the appropriate account administrator. Users who violate this policy will be subjected to disciplinary action.

Staff/students must follow the rules of network etiquette (netiquette). In addition, they must be polite, follow the organization's electronic writing and content guidelines, and use the network and Internet facility legally and appropriately.

LEGITIMATE USE

The School's IT facilities must not be used in any way that breaks the law or breaches Council standards.

Such breaches include, but are not limited to:

- making, distributing or using unlicensed software or data;
- making or sending threatening, offensive, or harassing messages;
- creating, possessing or distributing obscene material;
- unauthorized personal use of the School's computer facilities.

GUIDELINES OF IT POLICY

- Authentication of IT resources
  To protect the IT resources from unauthorized use, School must protect them and support regulations governing the privacy and security of sensitive data by using electronic identifiers and secure passwords to control access.
  To avoid unauthorized access, users (all categories) must follow specific rules for creating and using complex passwords. Password policy can be referred for what all requirements need to make the password complex.
- Mass E-mailing
  An email directed to any or all of the following: teachers, staff (academic and nonacademic), students, and alumni. Whosoever wishes to send the mass email must take permission from the higher administration top officials, along with the consent of staff and faculty members (included).

DATA BACKUP

The official and academic data backups have been done in the cloud.

One option is Google Drive, which is a complete Data management solution. The following steps will be adhered to by all while using the Google drive.

• Download Google drive on your PC to keep files in sync with your files stored on the web.

• Desktop version can be downloaded: http://www.google.co.in/drive/download at Carry out the two-step verification for security purposes.

• This facility is to be used only for Academic purposes/official documents and not for recreational/personal requirements like songs, movies, personal photographs etc.

CONFIDENTIAL INFORMATION

Employees may have access to confidential information about the School once written approval is granted. With the permission of management, employees may use email to communicate

confidential information internally to those with a need to know. Such email must be marked "confidential." When in doubt, do not use email to communicate confidential material. When a personal matter, it may be more appropriate to send a hard copy, place a phone call, or meet in person.

PRIVACY

Network and Internet access are provided as a tool to accomplish the organization's strategic goals and objectives. The School reserves the right to monitor, inspect, copy, review, and store at any time and without prior information, all network and Internet use, as well as all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this use. All such information, content, and files are the property of the School. Network administrators may review files and intercept communications for any reason, including, but not limited to, maintaining system integrity and ensuring staff/students are using the system in accordance with this policy.

SECURITY MEASURES

Physical security:

- Location Access: To protect resources such as keys, doors, and rooms maintained to the level of security with the value of the resources stored in those locations. Adequate consideration should be given to the physical security of ICT equipment rooms (including associated cabling). The server rooms should be locked when open access, by parents, for example, is in progress. The IT admin must ensure appropriate arrangements are applied to remove any ICT equipment from its usual location. These arrangements should consider the risks associated with the removal and the impact these risks might have.
- Equipment siting: Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users should observe the following precautions:
  - devices are positioned so that information stored or processed cannot be viewed by persons not authorized to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
  - equipment is sited to avoid environmental damage from causes such as dust & heat;
  - Users have been instructed to avoid leaving computers logged on when unattended if unauthorized access to the data can be gained. Clear written instructions to this effect should be given to users;
  - users have been instructed not to leave hard copies of sensitive data unattended on desks.

The same rules apply when accessing the School's IT System or IT data away from the School, e.g. at a User's home or visiting another school.

- Inventory: The Principal, in accordance with the School's Financial Regulations, shall ensure that an inventory of all IT equipment is maintained and all items accounted for at

least annually.

Administrative security: to protect resources such as:

- Full implementation of the most current authentication and authorization technologies.
- Most recently tested and approved software patches available.
- Most current and available security configurations.
- Most contemporary and available virus protection.
- Configuration of secure passwords on all IT devices

ACCEPTABLE USE POLICY

The School's Acceptable Use Policy applies to all school staff, students and third parties who use either or both of these facilities. The policy covers the use of Email, the Internet, services accessed through the Internet and local file and network usage. The conditions of use are explained in the policy. All school staff accessing these facilities must be issued with a copy of the 'Acceptable Use Policy and other relevant documents and complete the user declaration attached to the policy. For all students, the School will ensure that the appropriate 'Acceptable Use Policy' document is issued and students and their parents complete the consent form. In addition, copies of the 'Acceptable Use Policy' document and consent form will be given to all visitors.

PERSONAL USE

- The School has devoted time and effort to developing IT systems to assist you with your work. It is, however, recognized that there are times when you may want to use the Systems for non-work related purposes, and in recognition of this need, the School permits you to use the Systems for personal use.
- You must not use the systems for personal use during working hours. You must not allow personal use of systems to interfere with your day to day duties. Any non-job-related use of the systems during working hours may be subject to disciplinary action.
- You must not use School software for personal use unless the licence terms permit this, and you are responsible for checking the licensing position.
- Use of the systems should be strictly in accordance with all the related policies. In addition, you must pay all costs associated with personal use at the School's current rates, e.g. cost of paper.

NONCOMPLIANCE

- The use of the computer network and the Internet is a privilege, not a right. Violation of this policy, at the minimum, will lead to disciplinary action. Policy breaches include violating the above provisions and failing to report violations by other users. Permitting another person to use your account or password to access the network or the Internet, including, but not limited to, someone whose access has been denied or terminated, is a violation of policy. If another user violates this policy using one's account, the account holder will be held

responsible, and both will be subject to disciplinary/administrative action.

DISCIPLINARY IMPLICATIONS

Breaches of this policy may result in disciplinary action up to and including dismissal. They may also result in you being prosecuted, may lead to prosecution of the School and the individual(s) concerned or civil claims for damages.

SIGNED (CHAIRMAN)

SIGNED (PRINCIPAL)