IT-Cybersecurity Policy

Elite International School recognizes the value of technology security and values the need for a clear and consistent technology security policy, in compliance with legal and regulatory mandates, that promotes awareness and communicates expectations for safeguarding and securing its technology.

The purpose of this policy is to provide requirements for maintaining the confidentiality, integrity, availability, and accountability of EIS technology resources and data. The policy will address protection of EIS technology, access controls, technology equipment inventory management, network security, physical security, configuration management, and data security.

Protection of EIS Technology

1. EIS reserves the right to take all necessary legal actions to protect the confidentiality, integrity, availability, and accountability of its technology and to prevent its technology from being used for malicious activities.

2. Use of EIS technology to gain or attempt to gain unauthorized access to any system or information is prohibited.

3. EIS reserves the right, in accordance with legal and regulatory mandates, to monitor, archive, audit, or purge the contents of electronic communications, files, and other material created or stored using EIS technology, or data transmitted over EIS networks.

4. EIS reserves the right, in accordance with legal and regulatory mandates and as authorized by the Senior Management team/Managing Director, to access or disclose, for investigative purposes, the contents of electronic communications, files, and other material created or stored using EIS technology or data transmitted over EIS networks.

5. Failure by any individual using EIS technology to comply with this policy will result in the temporary or permanent restriction of technology access privileges, in addition to any applicable disciplinary actions or financial obligations.

Access Controls

1. Individuals using EIS technology will authenticate using individual account credentials. Exceptions will be approved by the Senior Management team/Managing Director

2. Individuals are prohibited from sharing EIS assigned account credentials unless permitted by the Senior Management team/Managing Director.

3. Individuals are granted access to EIS data and resources based on a least privilege methodology.

4. Access to EIS technology, granted by virtue of the individual’s role, will be terminated when the individual’s role is fulfilled or terminated.

Technology Equipment Accountability

1. All EIS technology equipment will be accounted for and tracked by location and functionality in an automated system before distribution.

2. EIS technology equipment will be audited periodically to ensure consistency and accuracy of the automated inventory system.

Network Security

All EIS technology networks will be designated as open or restricted.

1. Restricted EIS technology networks will be configured to protect against unauthorized access.
2. Individuals are prohibited from connecting non-EIS technology to restricted EIS networks without prior approval from the Senior Management team/Managing Director.
3. Individuals may connect non-EIS technology to open wireless EIS technology networks in accordance with Responsible Use of Technology and Social Media Policy.

Physical Security

1. Physical access to data centers, main distribution frames (MDFs), and intermediate distribution frames (IDFs) will be controlled to prevent and detect unauthorized access to these areas. Access to these areas will be granted to those persons who have legitimate responsibilities in those areas.

2. All data centers will be secured using technologies that monitor individual access and provide auditable access logs.

3. Individuals responsible for EIS technology must take reasonable steps to ensure the physical security of EIS technology.

Configuration Management

1. EIS technology system will be evaluated and monitored for appropriate security controls and effectiveness and approved by the Senior Management team/Managing Director.

2. EIS technology system will be monitored to confirm configuration and to determine the effectiveness of security controls.

3. All changes, including methods for transmitting and storing confidential data, will be approved and documented by the Senior Management team/Managing Director.

4. The Senior Management team/Managing Director will maintain a process for creating, managing, and documenting account credentials.

Electronic Communications

1. Individuals will have no expectation of personal privacy or confidentiality of any electronic communication when using EIS technology.

2. EIS technologies that store or transmit employee data, student record data, financial data, or other legally confidential data will implement appropriate authentication and encryption technologies to prevent unauthorized access or modification.

3. Individuals using EIS technology will ensure that both their usage and electronic communications content are in compliance with all other EIS policies.

Technology Security Incident Response

1. All EIS technology security investigations will be authorized by the Senior Management team/Managing Director.

2. EIS will monitor its technology for potential security incidents.

3. EIS reserves the right to access, record, restrict, or remove any content or device suspected of contributing to a security incident, with prior written approval from the Senior Management team/Managing Director. All security investigations will be documented by the Senior Management team.

4. The Senior Management team/Managing Director will conduct all EIS technology security incident investigations in strict confidence.

5. Investigations into incidents involving a potential breach of an individual's private data will include the following:

- Notifications to individuals will be required if it is determined that an individual’s personal information has been breached and misuse has occurred or is likely to occur.

- If misuse is not likely to occur, as in cases where the information breached was protected by encryption and there is no evidence the encryption key had been compromised or disclosed, notifications to individuals will not be required.

Storage Media Handling and Disposal

1. Access to EIS storage media including, but not limited to, floppy disks, magnetic tapes, hard disks, CDs, DVDs, USB memory sticks, etc., will be secured utilizing the least privileges methodology.

2. All service to EIS computers and servers will be performed onsite by authorized EIS personnel or authorized contractors. If a computer or server must be taken offsite for service, all hard drives, CDs, and DVDs will be removed prior to the equipment leaving the premises. If removal of any/all hard disks, CDs, or DVDs is not feasible, prior approval will be obtained in writing by the Senior Management team/Managing Director to remove the equipment.

3. All EIS storage media including, but not limited to, floppy disks, hard disks, CDs, DVDs, USB memory sticks, etc., will be disposed of in accordance with the school requirements.

System Security

1. EIS will employ technology security measures, including monitoring, to ensure the confidentiality, integrity, availability, and accountability of its technology and data.

2. Open wireless networks will be configured to notify users of network monitoring capabilities and the provisions of Responsible Use of Technology and Social Media Policy.

3. Individuals shall not attempt to circumvent, modify, or disable technology security measures implemented by EIS. These measures include but are not limited to:

- Anti-malware software
- Internet content filter
- Network firewalls
- Computer and server administrative management software

4. Wireless access points will be configured utilizing at least Wi-Fi Protected Access (WPA) encryption.

Account Credential Assignment and Use

1. Credential Assignment

- EIS employees and students will be assigned individual account credentials once their association with EIS has been verified.
- Account credentials are role-based and will be revoked when the individual's role is fulfilled or terminated.

2. Password Requirements

- Passwords will meet established length and complexity requirements and will not match the account username.
- Temporary passwords must be changed upon first login.
- Passwords will expire at regular intervals, and account credentials will be modified as necessary, based on changes in employment or enrollment status.

3. Shared Account Credentials (credentials used by more than a single individual)

- EIS may create shared account credentials in support of specific tasks with the approval of the Senior Management team/Managing Director.
- Shared accounts will only be used for the specific tasks for which they were intended.

Violations of the Policy

A. Any individual who suspects a violation of this policy or these implementation procedures will report the alleged violation to the Senior Management team for investigation.

B. The Senior Management team will report the suspected violation to the Managing Director for further investigation and potential disciplinary action.

C. In cases that may be criminal in nature (threats, stalking, harassment, etc.) or that may pose a safety threat, an investigation will be conducted in consultation and cooperation with the Senior Management team/Managing Director.

D. In cases of probable or potential harm to an individual, appropriate follow-through and communication with the individual in danger and others who are in a position to protect that individual from harm including, but not limited to the police, if necessary, must be undertaken by the individual who discovers the probable or potential harm.

E. Suspicious activity can be reported anonymously through the suggestion/complaint box.

Responsible Use of Technology and Social Media Policy

The school expects that all individuals will act in a responsible, civil, ethical, and appropriate manner when using technology for EIS-sanctioned activities.

The purpose of this policy is to define expectations for:

- The responsible use of technology and social media for EIS-sanctioned activities.
- The responsible use of technology and social media to enhance EIS process and improve system wide communications efforts.
- Maintaining the safety and privacy of individuals.

Compliance

1. Electronic students' and personnel's records, as well as other students' records and personally identifiable information, will be kept confidential and secure.
2. All digital tools and social media used with students for EIS-sanctioned activities will be authorized before use in accordance with the selection of instructional materials.
3. EIS technology and authorized digital tools and social media are accessible for instructional use and EIS-sanctioned activities consistent with current students' and employees' roles and instructional requirements.
4. All EIS technology, digital tools, and social media will comply with licensing and fair use agreements and applicable policies. Individuals will abide by the terms of service and privacy policy.
5. All authorized digital tools will comply with the state's law, protecting children's privacy.

7. In order to comply with the state's law and protects children's privacy:

a. EIS will deploy technology that attempts to filter abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material that is harmful to minors.

b. Employees will monitor online EIS-sanctioned students' activities including social media and digital tools, to the extent practical.

8. Staff will provide ongoing instruction to students concerning responsible, appropriate, and civil online behavior, including interacting with other individuals on social networking websites and in chat rooms, and regarding cyberbullying awareness and response.

9. Staff is prohibited from requesting or requiring an employee or applicant for employment to disclose any account credentials used for accessing a personal social media account or service.

Professional Use

1. Professional social media accounts created by employees are the property of EIS.

2. An employee must relinquish information necessary to maintain a professional social media account and may no longer access the account if the employee's job responsibilities change or employment is discontinued through resignation, retirement, termination, or any other cause.

Accountability

1. The destruction or theft of EIS technology as the result of negligence or misuse will be the financial responsibility of the responsible individual(s).

2. Individuals assume full responsibility for personally owned technology devices; therefore, EIS is not responsible for any personally owned technology devices.

3. Digital tools and social media used for EIS-sanctioned activities may be monitored for appropriate use. EIS may also access, monitor, archive, audit, purge or disclose the public contents of material created, stored or accessed through personal digital tools and social media accounts when possible and permitted by law.

4. EIS reserves the right to enable or disable interactive features on social media and to remove content inconsistent with the stated purpose, mission, and guidelines posted for the use of the social media.

5. Failure by any individual to comply with this policy may result in the temporary or permanent termination of technology access privileges, in addition to any applicable disciplinary action or financial obligation.

Individual Responsibilities

1. Individuals will take reasonable precautions to protect EIS owned technology equipment against damage, theft, and/or loss. If necessary, individuals will follow the appropriate process and/or procedure for reporting damage, theft, and/or loss.

2. Individuals will not engage in unauthorized activities. These include, but are not limited to:

   a. Accessing information for which the individuals do not have privilege

   b. Knowingly deploying computer viruses or software with malicious intent

   c. Violating copyright laws or privacy rights of others

   d. Plagiarizing

   e. Accessing EIS-owned technology via another individual's account credentials

   f. Damaging EIS technology

   g. Circumventing or disabling technology protection measures put in place by the SMT/Managing Director

3. Individuals will secure and safeguard data stored on EIS technology.

4. Individuals using digital tools and social media for EIS-sanctioned activities will use the most restrictive privacy settings when appropriate and available.

5. Individuals using EIS technology will not intentionally create, access, share, download or print content that:

   a. Depicts profanity, obscenity, the use of weapons, terrorism, or violence

   b. Promotes use of tobacco, drugs, alcohol, or other illegal or harmful products

   c. Contains sexually suggestive messages

   d. Is sexually explicit or obscene

   e. Depicts gang affiliation

   f. Contains language or symbols that demean an identifiable person or group or otherwise infringe on the rights of others

   g. Causes or is likely to cause a disruption to EIS activities or the orderly operation of EIS

   h. Contains rude, disrespectful, or discourteous expressions inconsistent with civil discourse or behavior.

   i. Constitutes bullying, cyberbullying, harassment, or intimidation.

   j. Reasonable exceptions to this provision may be made for students conducting research under the direction of an instructor and employees completing EIS related responsibilities. Specific permission will be granted regarding the nature of the research to be conducted and the type of files related to that research which might be accessed or created.

6. Individuals will authenticate using EIS active directory credential assigned to each individual, when using EIS owned or personally owned devices.

7. EIS has the following expectations for individuals using personally owned technology during EIS-sanctioned activities:

a. Individuals will use personally owned devices in accordance with all EIS policies. Failure to comply with these polices may result in the removal of temporary or permanent use privileges in addition to any disciplinary action.

b. Individuals will use devices in a responsible, civil, ethical, and legal manner.

c. Individuals will assume full responsibility for their personal technology devices and the content stored on these devices.

d. Individuals will ensure that their personal technology devices contain up to date operating system and relevant software patches and anti-malware software.

e. EIS will not be liable for any costs incurred related to the use of personal technology devices, including but not limited to, usage fees, upgrades, damages, and replacements.

f. Individuals will have no expectation of personal privacy or confidentiality of any electronic communication when using EIS networks.

g. Individuals will not store confidential EIS information, excluding the device owner's personal information, on personal technology devices.

h. Individuals will not use personal technology devices to create or access abusive, libelous, obscene, offensive, profane, threatening, sexually explicit, pornographic, illegal, or other inappropriate material during EIS-sanctioned activities.

i. Individuals will not use personal technology devices to gain or attempt to gain unauthorized access to any system or information.

j. Individuals will not use personal technology devices to circumvent, modify, or disable technology security measures implemented by EIS. These measures include but are not limited to:

- Anti-malware software
- Internet content filter
- Privacy settings and/or parental controls
- Network firewalls
- Computer and server administrative management software

k. Personal technology devices placed on EIS network may not disrupt normal network activities

l. Individuals are responsible for reporting any inappropriate material they receive on personal technology devices.

8. Employees selecting online resources will evaluate the resources to ensure that they meet the curricular needs of students and are appropriate for the developmental level of the students.

9. EIS employees will ensure students are authenticating to the network when using EIS-owned or personally owned devices.

10. Upon request, employees will provide the administration access to any professional social media accounts or forums they have created.

11. Any postings by employees will not reference, link or contain:

a. Statements that could be viewed as malicious, obscene, threatening or intimidating; that disparage students, employees, parents or community members; or that could be viewed as harassment or bullying.

b. EIS password-protected proprietary items, private, confidential or attorney-client privileged information such as assessments, and personnel issues.

12. Employees are responsible for all communication sent from their accounts. When using electronic accounts to correspond with parents and students, employees will use an approved EIS communication system.

13. Employees will ensure the confidentiality and privacy of student, staff and Ministry’s data. Employees will only share confidential data when directed to do so by the SMT/Managing Director.

14. Employees will ensure that when parents have requested that their students are not photographed, those students do not appear in EIS publications, including social media. This restriction does not apply to extracurricular events that are open to the public.

15. Employees will not use EIS logos or trademarks for personal use.

Violation of Policy

- Any individual who suspects a violation of this policy or these implementation procedures will report the alleged violation to the SMT for investigation.
- The Senior Management team will report the suspected violation to the Managing Director for further investigation and potential disciplinary action.
- In cases that may be criminal in nature (threats, stalking, harassment, etc.) or that may pose a safety threat, an investigation will be conducted in consultation and cooperation with the Managing Director.

Students' Guidelines for Using ICT

- Only use computers when a teacher is present to supervise.
- Do not modify, delete, or copy any programs, applications, or operating system files.
- Use only school-approved programs on the computers.
- Do not load, download, or install any software or programs on the computers or networks.
- Avoid moving, damaging, or attempting to damage any computer peripherals (e.g., mouse, keyboard, printer, speakers, microphone, headphone, CPU, monitor).
- Save data only to assigned locations; system space is limited and may be periodically cleared.
- Personal storage devices (USB flash drives, external hard disks, CDs, etc.) may only be used with approval from the ICT teacher.
- Non-educational games are prohibited at all times. If unsure whether a game is educational, consult your ICT lab teacher.
- Clean your workspace after use by straightening the mouse, keyboard, and pushing in your chair.
- Keep device volume muted unless using headphones.

- Log out of all web applications or e-portals when finished.
- Clean your hands before using the devices and refrain from touching them when the teacher is speaking. No food or drinks are allowed inside the lab.
- Practice typing at home to meet middle and high school expectations and enhance your experience with technology projects at EIS.

Online and Media Expectations

- Prioritize safety, respect, and responsibility in all online activities.
- Utilize school resources solely for educational purposes.
- Refrain from altering device settings.
- Only capture or record images or videos of students if explicitly instructed to do so.
- Report any technical issues or equipment problems to the ICT teacher immediately, rather than attempting to resolve them independently.

Focus on Learning - not Distracting

- All school accounts and devices are to be used exclusively for school-related activities. (No messaging or chatting for non-school purposes.)
- Stay on topic during all school-related tasks.
- Use proper writing; avoid junk typing or texting lingo.
- Ensure all images are educational and appropriate for school.
- Do NOT share answers for any assessments.

Our Digital Citizenship Pledge

- I will communicate responsibly and kindly with others.
- I will respect other's ideas and opinions.
- I will give proper credit when I use other's work.
- I will protect my own and other's private information.
- I will stand up to cyberbullying.
- I will avoid and report any harmful or inappropriate content I come across online.