

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 policies 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 with 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 students, 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 for cyberbullying.
- I will avoid and report any harmful or inappropriate content I come across online.

سياسة الأمن السيبراني لتكنولوجيا المعلومات

تدرك مدرسة النخبة العالمية قيمة الأمن التكنولوجي وتقدر الحاجة إلى سياسة أمنية تقنية واضحة ومتسقة، وفقا للإرشادات القانونية والتنظيمية، والتي تعزز الوعي وتنقل التوقعات لحماية وتأمين تقينتها.

الهدف من هذه السياسة هو توفير متطلبات للحفاظ على سرية وسلامة وتوافر ومساءلة موارد وبيانات تقنية لمدرسة النخبة العالمية. سنتناول السياسة حماية تقنية مدرسة النخبة العالمية، وضوابط الوصول، وإدارة مخزون المعدات التكنولوجية، وأمن الشبكة، والأمن المادي، وإدارة التكوين، وأمن البيانات.

حماية تقنية مدرسة النخبة العالمية

1. تحتفظ مدرسة النخبة العالمية بالحق في اتخاذ جميع الإجراءات القانونية اللازمة لحماية سرية تقينتها وسلامتها وتوافرها ومساءلتها ومنع استخدام تقينتها في أنشطة ضارة.
2. يحظر استخدام تقنية مدرسة النخبة العالمية للحصول على أو محاولة الوصول غير المصرح به إلى أي نظام أو معلومات.
3. تحتفظ مدرسة النخبة العالمية بالحق، وفقا للتفويضات القانونية والتنظيمية، في مراقبة أو أرشفة أو تدقيق أو تطهير محتويات الاتصالات الإلكترونية والملفات والمواد الأخرى التي تم إنشاؤها أو تخزينها باستخدام تقنية مدرسة النخبة العالمية أو البيانات المنقولة عبر شبكات مدرسة النخبة العالمية.
4. تحتفظ مدرسة النخبة العالمية بالحق، وفقا للتفويضات القانونية والتنظيمية وعلى النحو المصرح به من قبل فريق الإدارة العليا / العضو المنتدب، في الوصول أو الكشف، لأغراض التحقيق، عن محتويات الاتصالات الإلكترونية والملفات والمواد الأخرى التي تم إنشاؤها أو تخزينها باستخدام تقنية مدرسة النخبة العالمية أو البيانات المنقولة عبر شبكات مدرسة النخبة العالمية.
5. سيؤدي فشل أي فرد يستخدم تقنية مدرسة النخبة العالمية في الامتثال لهذه السياسة إلى تقييد مؤقت أو دائم لامتيازات الوصول إلى التكنولوجيا، بالإضافة إلى أي إجراءات تأديبية أو التزامات مالية سارية.

عناصر التحكم في الوصول

1. سيقوم الأفراد الذين يستخدمون تقنية EIS بالمصادقة باستخدام بيانات اعتماد الحساب الفردي. سيتم الموافقة على الاستثناءات من قبل فريق الإدارة العليا / العضو المنتدب.
2. يحظر على الأفراد مشاركة بيانات اعتماد الحساب المعينة من EIS ما لم يسمح بذلك فريق الإدارة العليا / العضو المنتدب.
3. يتم منح الأفراد حق الوصول إلى بيانات وموارد EIS بناء على منهجية أقل امتياز.
4. سيتم إنهاء الوصول إلى تقنية EIS، الممنوحة بحكم دور الفرد، عند الوفاء بدور الفرد أو إنهائه.

مساءلة المعدات التكنولوجية

1. سيتم حساب جميع معدات تقنية EIS وتتبعها حسب الموقع والوظائف في نظام آلي قبل التوزيع.
2. سيتم تدقيق معدات تقنية EIS بشكل دوري لضمان اتساق ودقة نظام المخزون الآلي.

أمن الشبكات

- سيتم تعيين جميع شبكات تقنية EIS على أنها مفتوحة أو مقيدة.
- سيتم تكوين شبكات تقنية EIS المقيدة للحماية من الوصول غير المصرح به.

- يحظر على الأفراد توصيل تقنية غير EIS بشبكات EIS المقيدة دون موافقة مسبقة من فريق الإدارة العليا / العضو المنتدب.
- يمكن للأفراد توصيل تقنية غير EIS لفتح شبكات تقنية EIS اللاسلكية وفقا لسياسة الاستخدام المسؤول للتكنولوجيا ووسائل التواصل الاجتماعي.

الأمن المادي

1. سيتم التحكم في الوصول المادي إلى مراكز البيانات وإطارات التوزيع الرئيسية (MDFs) وإطارات التوزيع الوسيطة (IDFs) لمنع واكتشاف الوصول غير المصرح به. وسيمنح الوصول إلى هذه المناطق للأشخاص الذين يتحملون مسؤوليات مشروعة.
2. سيتم تأمين جميع مراكز البيانات باستخدام التقنيات التي تراقب الوصول الفردي وتوفر سجلات وصول قابلة للتدقيق.
3. يجب على الأفراد المسؤولين عن تقنية مدرسة النخبة العالمية اتخاذ خطوات معقولة لضمان الأمن المادي لتقنية مدرسة النخبة العالمية.

إدارة التكوين

1. سيتم تقييم ومراقبة نظام تكنولوجيا مدرسة النخبة العالمية من أجل الضوابط الأمنية المناسبة والفعالية والموافقة عليها من قبل فريق الإدارة العليا / العضو المنتدب.
2. سيتم مراقبة نظام تقنية مدرسة النخبة العالمية لتأكيد التكوين وتحديد فعالية الضوابط الأمنية.
3. سيتم الموافقة على جميع التغييرات ، بما في ذلك طرق نقل وتخزين البيانات السرية ، وتوثيقها من قبل فريق الإدارة العليا / العضو المنتدب.
4. سيحافظ فريق الإدارة العليا / العضو المنتدب على عملية لإنشاء بيانات اعتماد الحساب وإدارتها وتوثيقها.

التواصل الإلكتروني

1. لن يتوقع الأفراد الخصوصية الشخصية أو سرية أي تواصل إلكتروني عند استخدام تقنية مدرسة النخبة العالمية.
2. ستقوم تقنيات مدرسة النخبة العالمية التي تخزن أو تنقل بيانات الموظفين أو بيانات سجل الطلاب أو البيانات المالية أو غيرها من البيانات السرية قانونا بتنفيذ تقنيات المصادقة والتشفير المناسبة لمنع الوصول أو التعديل غير المصرح به.
3. سيضمن الأفراد الذين يستخدمون تقنية مدرسة النخبة العالمية أن كل من استخدامهم ومحتوى الاتصالات الإلكترونية يتوافق مع جميع سياسات مدرسة النخبة العالمية الأخرى.

الاستجابة لحوادث أمن التكنولوجيا

1. سيتم تفويض جميع تحقيقات أمان تقنية مدرسة النخبة العالمية من قبل فريق الإدارة العليا / المدير العام.
2. ستقوم مدرسة النخبة العالمية بمراقبة تقنياتها بحثا عن الحوادث الأمنية المحتملة.
3. تحتفظ مدرسة النخبة العالمية بالحق في الوصول إلى أو تسجيل أو تقييد أو إزالة أي محتوى أو جهاز يشتبه في مساهمته في حادث أمني ، بموافقة كتابية مسبقة من فريق الإدارة العليا / العضو المنتدب. سيتم توثيق جميع التحقيقات الأمنية من قبل فريق الإدارة العليا.
4. سيقوم فريق الإدارة العليا / العضو المنتدب بإجراء جميع التحقيقات في حوادث أمن تكنولوجيا مدرسة النخبة العالمية بسرية تامة.
5. ستشمل التحقيقات في الحوادث التي تنطوي على خرق محتمل للبيانات الخاصة للفرد ما يلي:
 - ستكون هناك حاجة إلى إخطارات للأفراد إذا تم تحديد أن المعلومات الشخصية للفرد قد تم اختراقها وأن إساءة الاستخدام قد حدثت أو من المحتمل أن تحدث.
 - إذا لم يكن من المحتمل حدوث سوء استخدام، كما هو الحال في الحالات التي تكون فيها المعلومات التي تم اختراقها محمية بالتشفير ولا يوجد دليل على أن مفتاح التشفير قد تم اختراقه أو الكشف عنه، فلن تكون هناك حاجة إلى إخطارات للأفراد.

معالجة وسائط التخزين والتخلص منها

1. سيتم تأمين الوصول إلى وسائط تخزين مدرسة النخبة العالمية بما في ذلك ، على سبيل المثال لا الحصر ، الأقراص المرنة والأشرطة المغناطيسية والأقراص الصلبة والأقراص المضغوطة وأقراص DVD وشرائح ذاكرة USB وما إلى ذلك ، باستخدام منهجية أقل الامتيازات.
2. سيتم تنفيذ جميع الخدمات لأجهزة حاسوب مدرسة النخبة العالمية في الموقع من قبل موظفي مدرسة النخبة العالمية المعتمدين. إذا كان يجب إخراج جهاز حاسوب خارج الموقع للخدمة، إزالة جميع محركات الأقراص الثابتة والأقراص المضغوطة وأقراص DVD قبل مغادرة الجهاز للمبنى. إذا لم يكن من الممكن إزالة أي / جميع الأقراص الصلبة أو الأقراص المدمجة أو أقراص DVD ، الحصول على موافقة كتابية مسبقة من قبل فريق الإدارة العليا / المدير الإداري لإزالة المعدات.
3. سيتم التخلص من جميع وسائط تخزين مدرسة النخبة العالمية بما في ذلك ، على سبيل المثال لا الحصر ، الأقراص المرنة والأقراص الصلبة والأقراص المضغوطة وأقراص DVD وشرائح ذاكرة USB وما إلى ذلك ، وفقا لمتطلبات المدرسة.

أمن النظام

1. ستستخدم مدرسة النخبة العالمية تدابير أمان التكنولوجيا، بما في ذلك المراقبة ، لضمان سرية وسلامة وتوافر ومساءلة تقنياتها وبياناتها.
2. سيتم تكوين الشبكات اللاسلكية المفتوحة لإخطار المستخدمين بقدرات مراقبة الشبكة وأحكام سياسة الاستخدام المسؤول للتكنولوجيا ووسائل التواصل الاجتماعي.
3. لا يجوز للأفراد محاولة التحايل أو تعديل أو تعطيل تدابير أمان التكنولوجيا التي تنفذها مدرسة النخبة العالمية. وتشمل هذه التدابير على سبيل المثال لا الحصر:

- برامج مكافحة البرامج الضارة

- فلتر محتوى الإنترنت

- جدران حماية الشبكة

- برنامج الإدارة الإدارية للحاسوب

4. سيتم تكوين نقاط الوصول اللاسلكية باستخدام تشفير الوصول المحمي بشبكة (Wi-Fi (WPA على الأقل.

تعيين بيانات اعتماد الحساب واستخدامها

تعيين بيانات الاعتماد

- سيتم تعيين بيانات اعتماد حساب فردية لموظفي مدرسة النخبة العالمية والطلاب بمجرد التحقق من ارتباطهم بمدرسة النخبة العالمية.
- تستند بيانات اعتماد الحساب إلى الدور وسيتم إبطالها عند استيفاء دور الفرد أو إنهائه.

متطلبات كلمة المرور

- ستبلي كلمات المرور متطلبات الطول والتعقيد المحددة ولن تتطابق مع اسم مستخدم الحساب.
- يجب تغيير كلمات المرور المؤقتة عند تسجيل الدخول لأول مرة.
- ستتتهي صلاحية كلمات المرور على فترات منتظمة، وسيتم تعديل بيانات اعتماد الحساب حسب الضرورة، بناء على التغييرات في حالة التوظيف أو التسجيل.

بيانات اعتماد الحساب المشترك (بيانات الاعتماد المستخدمة من قبل أكثر من فرد واحد)

- يجوز لمدرسة النخبة العالمية إنشاء بيانات اعتماد حساب مشتركة لدعم مهام محددة بموافقة فريق الإدارة العليا / العضو المنتدب.
- سيتم استخدام الحسابات المشتركة فقط للمهام المحددة التي كانت مخصصة لها.

انتهاكات السياسة

- أ. أي فرد يشتبه في انتهاك هذه السياسة أو إجراءات التنفيذ هذه سيقوم بالإبلاغ عن الانتهاك المزعوم إلى فريق الإدارة العليا للتحقيق فيه.
- ب. سيقوم فريق الإدارة العليا بإبلاغ المدير العام عن الانتهاك المشتبه به لمزيد من التحقيق واتخاذ إجراءات تأديبية محتملة.
- ج. في الحالات التي قد تكون ذات طبيعة إجرامية (التحديات، المطاردة، المضايقة، إلخ) أو التي قد تشكل تهديدا للسلامة، سيتم إجراء تحقيق بالتشاور والتعاون مع فريق الإدارة العليا.
- د. في حالات الضرر المحتمل أو المحتمل للفرد، يجب أن يقوم الفرد الذي يكتشف الضرر المحتمل بالمتابعة والتواصل المناسبين مع الفرد المعرض للخطر وغيره ممن هم في وضع يسمح لهم بحماية هذا الفرد من الأذى بما في ذلك، على سبيل المثال لا الحصر، الشرطة، إذا لزم الأمر، من قبل الفرد الذي يكتشف الضرر المحتمل.
- هـ. يمكن الإبلاغ عن النشاط المشبوه بشكل مجهول من خلال صندوق الاقتراح / الشكوى.

سياسة الاستخدام المسؤول للتكنولوجيا ووسائل التواصل الاجتماعي

تتوقع المدرسة أن يتصرف جميع الأفراد بطريقة مسؤولة ومدنية وأخلاقية ومناسبة عند استخدام التكنولوجيا للأنشطة التي تقرها مدرسة النخبة العالمية.

الغرض من هذه السياسة هو تحديد التوقعات لما يلي:

- الاستخدام المسؤول للتكنولوجيا ووسائل التواصل الاجتماعي للأنشطة التي تقرها مدرسة النخبة العالمية.
- الاستخدام المسؤول للتكنولوجيا ووسائل التواصل الاجتماعي لتعزيز عملية مدرسة النخبة العالمية وتحسين جهود الاتصالات على مستوى النظام.
- المحافظة على سلامة وخصوصية الأفراد.

الامتثال

- سيتم الاحتفاظ بسجلات الطلاب والموظفين الإلكترونية، بالإضافة إلى سجلات الطلاب الآخرين ومعلومات التعريف الشخصية، بسرية وأمان.
 - سيتم التصريح بجميع الأدوات الرقمية ووسائل التواصل الاجتماعي المستخدمة مع الطلاب للأنشطة المعتمدة من مدرسة النخبة العالمية قبل الاستخدام وفقا لاختيار المواد التعليمية.
 - يمكن الوصول إلى تقنية مدرسة النخبة العالمية والأدوات الرقمية المعتمدة ووسائل التواصل الاجتماعي للاستخدام التعليمي والأنشطة المعتمدة من مدرسة النخبة العالمية بما يتفق مع أدوار الطلاب والموظفين الحاليين والمتطلبات التعليمية.
 - ستتوافق جميع تقنيات مدرسة النخبة العالمية والأدوات الرقمية ووسائل التواصل الاجتماعي مع اتفاقيات الترخيص والاستخدام العادل والسياسات المعمول بها. يلتزم الأفراد بشروط الخدمة وسياسة الخصوصية.
 - ستتوافق جميع الأدوات الرقمية المصرح بها مع قانون الدولة، مما يحمي خصوصية الأطفال.
7. من أجل الامتثال لقانون الدولة وحماية خصوصية الأطفال:

أ. ستنتشر مدرسة النخبة العالمية تقنية تحاول تصفية المواد المسيئة، أو التشهيرية، أو البذيئة أو التهديدية أو الإباحية أو غير القانونية أو غيرها من المواد غير اللائقة الضارة بالقصر.

ب. سيقوم الموظفون بمراقبة أنشطة الطلاب عبر الإنترنت المعتمدة من مدرسة النخبة العالمية بما في ذلك وسائل التواصل الاجتماعي والأدوات الرقمية، إلى الحد العملي.

8. سيقدم الموظفون تعليمات مستمرة للطلاب فيما يتعلق بالسلوك المسؤول والمناسب والمدني عبر الإنترنت ، بما في ذلك التفاعل مع الأفراد الآخرين على مواقع الشبكات الاجتماعية وفي غرف الدردشة ، وفيما يتعلق بالتوعية والاستجابة للتنمر عبر الإنترنت.

9. يحظر على الموظفين طلب أو مطالبة الموظف أو مقدم الطلب للتوظيف بالكشف عن أي بيانات اعتماد للحساب تستخدم للوصول إلى حساب أو خدمة شخصية على وسائل التواصل الاجتماعي.

الاستخدام المهني

1. حسابات وسائل التواصل الاجتماعي المهنية التي أنشأها الموظفون هي ملك لمدرسة النخبة العالمية.
2. يجب على الموظف التخلي عن المعلومات اللازمة للحفاظ على حساب احترافي على وسائل التواصل الاجتماعي ولا يجوز له الوصول إلى الحساب إذا تغيرت مسؤوليات الوظيفة للموظف أو توقف العمل من خلال الاستقالة أو التقاعد أو إنهاء الخدمة أو أي سبب آخر.

المساءلة

1. سيكون تدمير أو سرقة تقنية مدرسة النخبة العالمية نتيجة للإهمال أو سوء الاستخدام مسؤولية مالية للفرد (الأفراد) المسؤول.
2. يتحمل الأفراد المسؤولية الكاملة عن أجهزة التكنولوجيا المملوكة شخصيا ؛ لذلك ، فإن مدرسة النخبة العالمية ليست مسؤولة عن أي أجهزة تقنية مملوكة شخصيا.
3. يمكن مراقبة الأدوات الرقمية ووسائل التواصل الاجتماعي المستخدمة في الأنشطة التي تقرها مدرسة النخبة العالمية للاستخدام المناسب. يجوز لمدرسة النخبة العالمية أيضا الوصول إلى المحتويات العامة للمواد التي تم إنشاؤها أو تخزينها أو الوصول إليها من خلال الأدوات الرقمية الشخصية وحسابات وسائل التواصل الاجتماعي، أو مراقبتها أو أرشفتها أو تدقيقها أو تطهيرها أو الكشف عنها عندما يكون ذلك ممكنا ويسمح به القانون.
4. تحتفظ مدرسة النخبة العالمية بالحق في تمكين أو تعطيل الميزات التفاعلية على وسائل التواصل الاجتماعي وإزالة المحتوى الذي لا يتوافق مع الغرض والمهمة والإرشادات المعلنة المنشورة لاستخدام وسائل التواصل الاجتماعي.
5. قد يؤدي فشل أي فرد في الامتثال لهذه السياسة إلى الإنهاء المؤقت أو الدائم لامتيازات الوصول إلى التكنولوجيا ، بالإضافة إلى أي إجراء تأديبي أو التزام مالي ساري المفعول.

المسؤوليات الفردية

1. سيتخذ الأفراد الاحتياطات المعقولة لحماية معدات التكنولوجيا المملوكة لمدرسة النخبة العالمية من التلف و / أو السرقة و / أو الخسارة. إذا لزم الأمر ، سيتبع الأفراد العملية و / أو الإجراء المناسب للإبلاغ عن الضرر و / أو السرقة و / أو الخسارة.
2. لن يشارك الأفراد في أنشطة غير مصرح بها. وتشمل هذه، على سبيل المثال لا الحصر:
 - الوصول إلى المعلومات التي لا يتمتع الأفراد بامتياز لها
 - نشر فيروسات الكمبيوتر أو البرامج عن قصد بقصد ضار
 - انتهاك قوانين حقوق الطبع والنشر أو حقوق الخصوصية للآخرين
 - يغشون
 - الوصول إلى التكنولوجيا المملوكة لشركة مدرسة النخبة العالمية عبر بيانات اعتماد حساب فرد آخر
 - إتلاف تقنية مدرسة النخبة العالمية
 - التحايل على تدابير حماية التكنولوجيا أو تعطيلها التي يضعها فريق الإدارة العليا/ المدير العام
3. سيقوم الأفراد بتأمين وحماية البيانات المخزنة على تقنية مدرسة النخبة العالمية.
4. سيستخدم الأفراد الذين يستخدمون الأدوات الرقمية ووسائل التواصل الاجتماعي للأنشطة التي تقرها مدرسة النخبة العالمية إعدادات الخصوصية الأكثر تقييدا عندما يكون ذلك مناسباً ومتاحاً.
5. لن يقوم الأفراد الذين يستخدمون تقنية مدرسة النخبة العالمية عن قصد بإنشاء محتوى أو الوصول إليه أو مشاركته أو تنزيله أو طباعته:
 - أ. يصور الألفاظ النابية، أو الفحش، أو استخدام الأسلحة أو الإرهاب أو العنف
 - ب. يروج لاستخدام التبغ، أو المخدرات، أو الكحول أو غيرها من المنتجات غير القانونية أو الضارة
 - ج. يحتوي على رسائل موحية جنسيا
 - د. يحتوي على تصريح جنسي أو فاحش
 - هـ. يصور الانتماء إلى عصابة

- و. يحتوي على لغة أو رموز تحط من قدر شخص أو مجموعة يمكن التعرف عليها أو تنتهك حقوق الآخرين
- ز. يسبب أو من المحتمل أن يتسبب في تعطيل أنشطة مدرسة النخبة العالمية أو التشغيل المنظم لمدرسة النخبة العالمية
- ح. يحتوي على تعبيرات وقحة أو غير محترمة أو غير مهذبة لا تتفق مع الخطاب أو السلوك المدني.
- ط. بشكل تملأ أو تملأ عبر الإنترنت أو مضايقة أو ترهيباً.
- ي. قد يتم إجراء استثناءات معقولة لهذا الحكم للطلاب الذين يجرون أبحاثاً تحت إشراف مدرس وموظفين يكملون المسؤوليات المتعلقة بمدرسة النخبة العالمية. سيتم منح إذن محدد فيما يتعلق بطبيعة البحث الذي سيتم إجراؤه ونوع الملفات المتعلقة بهذا البحث والتي يمكن الوصول إليها أو إنشاؤها.
6. سيقوم الأفراد بالمصادقة باستخدام بيانات اعتماد الدليل النشط مدرسة النخبة العالمية المعينة لكل فرد، عند استخدام الأجهزة المملوكة أو المملوكة لمدرسة النخبة العالمية شخصياً.
7. لدى مدرسة النخبة العالمية التوقعات التالية للأفراد الذين يستخدمون التكنولوجيا المملوكة شخصياً أثناء الأنشطة التي تقرها مدرسة النخبة العالمية:
 - أ. سيستخدم الأفراد الأجهزة المملوكة شخصياً وفقاً لجميع سياسات مدرسة النخبة العالمية. قد يؤدي عدم الامتثال لهذه السياسات إلى إزالة امتيازات الاستخدام المؤقت أو الدائم بالإضافة إلى أي إجراء تأديبي.
 - ب. سيستخدم الأفراد الأجهزة بطريقة مسؤولة، ومدنية وأخلاقية وقانونية.
 - ج. يتحمل الأفراد المسؤولية الكاملة عن أجهزتهم التقنية الشخصية والمحتوى المخزن على هذه الأجهزة.
 - د. سيضمن الأفراد أن أجهزتهم التقنية الشخصية تحتوي على نظام تشغيل محدث وتحديثات البرامج ذات الصلة وبرامج مكافحة البرامج الضارة.
 - هـ. لن تكون مدرسة النخبة العالمية مسؤولة عن أي تكاليف يتم تكبدها فيما يتعلق باستخدام أجهزة التكنولوجيا الشخصية، بما في ذلك على سبيل المثال لا الحصر، رسوم الاستخدام، والترقيات والأضرار والاستبدال.
 - و. لن يتوقع الأفراد الخصوصية الشخصية أو سرية أي اتصال إلكتروني عند استخدام شبكات مدرسة النخبة العالمية.
 - ز. لن يقوم الأفراد بتخزين معلومات مدرسة النخبة العالمية السرية، باستثناء المعلومات الشخصية لمالك الجهاز، على أجهزة التكنولوجيا الشخصية.
 - ح. لن يستخدم الأفراد أجهزة التكنولوجيا الشخصية لإنشاء أو الوصول إلى مواد مسيئة أو تشهيرية أو فاحشة أو مسيئة أو مدسنة، أو تهديدية أو جنسية صريحة أو إباحية أو غير قانونية أو غيرها من المواد غير اللائقة أثناء الأنشطة التي تقرها مدرسة النخبة العالمية.
 - ط. لن يستخدم الأفراد أجهزة التكنولوجيا الشخصية للحصول أو محاولة الوصول غير المصرح به إلى أي نظام أو معلومات.
 - ي. لن يستخدم الأفراد أجهزة التكنولوجيا الشخصية للتحايل على تدابير أمان التكنولوجيا التي تنفذها مدرسة النخبة العالمية أو تعديلها أو تعطيلها. وتشمل هذه التدابير على سبيل المثال لا الحصر:
 - برامج مكافحة البرامج الضارة
 - تصفية محتوى الإنترنت
 - إعدادات الخصوصية و / أو الرقابة الأبوية
 - جدران حماية الشبكة
 - برامج الإدارة الإدارية للحاسوب
 - ك. قد لا تعطل أجهزة التكنولوجيا الشخصية الموضوع على شبكة مدرسة النخبة العالمية أنشطة الشبكة العادية.
 - ل. الأفراد مسؤولون عن الإبلاغ عن أي مواد غير لائقة يتلقونها على أجهزة التكنولوجيا الشخصية.
8. سيقوم الموظفون الذين يختارون الموارد عبر الإنترنت بتقييم الموارد للتأكد من أنها تلبي احتياجات المناهج الدراسية للطلاب ومناسبة للمستوى التنموي للطلاب.
9. سيضمن موظفو مدرسة النخبة العالمية مصادقة الطلاب على الشبكة عند استخدام الأجهزة المملوكة لمدرسة النخبة العالمية أو المملوكة شخصياً.
10. عند الطلب، سيوفر الموظفون للإدارة إمكانية الوصول إلى أي حسابات أو منتديات مهنية على وسائل التواصل الاجتماعي قاموا بإنشائها.
11. أي منشورات من قبل الموظفين لن تشير أو تربط أو تحتوي على:
 - أ. التصريحات التي يمكن اعتبارها خبيثة، أو فاحشة، أو تهديدية، أو مخيفة؛ التي تحط من قدر الطلاب، أو الموظفين، أو أولياء الأمور، أو أفراد المجتمع؛ أو يمكن اعتباره مضايقة أو تملأ.

ب. عناصر الملكية المحمية بكلمة مرور مدرسة النخبة العالمية، والمعلومات الخاصة أو السرية أو المميزة بين المحامي والعميل مثل التقييمات وقضايا الموظفين.

12. الموظفون مسؤولون عن جميع الاتصالات المرسله من حساباتهم. عند استخدام الحسابات الإلكترونية للمراسلة مع أولياء الأمور والطلاب، سيستخدم الموظفون نظام اتصال مدرسة النخبة العالمية معتمد.

13. يحرص الموظفون على سرية وخصوصية بيانات الطلاب والموظفين والوزارة. لن يشارك الموظفون البيانات السرية إلا عندما يوجههم ذلك فريق الإدارة العليا / المدير العام.

14. سيضمن الموظفون أنه عندما يطلب أولياء الأمور عدم تصوير طلابهم، فإن هؤلاء الطلاب لا يظهرون في منشورات مدرسة النخبة العالمية، بما في ذلك وسائل التواصل الاجتماعي. لا ينطبق هذا القيد على الأحداث اللامنهجية المفتوحة.

15. لن يستخدم الموظفون شعارات مدرسة النخبة العالمية أو العلامات التجارية للاستخدام الشخصي.

انتهاك السياسة

- أي فرد يشتبه في حدوث انتهاك لهذه السياسة أو إجراءات التنفيذ هذه سوف يبلغ عن الانتهاك المزعوم إلى فريق الإدارة العليا للتحقيق.
- سيقوم فريق الإدارة العليا بإبلاغ المدير العام عن الانتهاك المشتبه به لمزيد من التحقيق واتخاذ إجراءات تأديبية محتملة.
- في الحالات التي قد تكون ذات طبيعة إجرامية (التهديدات، المطاردة، المضايقة، إلخ) أو التي قد تشكل تهديدا للسلامة، سيتم إجراء تحقيق بالتشاور والتعاون مع المدير العام.

إرشادات الطلاب لاستخدام تكنولوجيا المعلومات والاتصالات

- استخدم أجهزة الكمبيوتر فقط عندما يكون المعلم حاضرا للإشراف.
- لا تقم بتعديل أو حذف أو نسخ أي برامج أو تطبيقات أو ملفات نظام التشغيل.
- استخدم فقط البرامج المعتمدة من المدرسة على أجهزة الكمبيوتر.
- لا تقم بتحميل أو تنزيل أو تثبيت أي برامج أو برامج على أجهزة الكمبيوتر أو الشبكات.
- تجنب تحريك أو إتلاف أو محاولة إتلاف أي من الأجهزة الطرفية للكمبيوتر (مثل الماوس ولوحة المفاتيح والطابعة ومكبرات الصوت والميكروفون وسماعة الرأس ووحدة المعالجة المركزية والشاشة).
- حفظ البيانات فقط في المواقع المخصصة؛ مساحة النظام محدودة ويمكن إفراغها بشكل دوري.
- لا يجوز استخدام أجهزة التخزين الشخصية (محركات أقراص USB المحمولة والأقراص الصلبة الخارجية والأقراص المدمجة وما إلى ذلك) إلا بموافقة مدرس تكنولوجيا المعلومات والاتصالات.
- الألعاب غير التعليمية محظورة في جميع الأوقات. إذا لم تكن متأكدا مما إذا كانت اللعبة تعليمية، فاستشر مدرس مختبر تكنولوجيا المعلومات والاتصالات الخاص بك.
- نظف مساحة العمل الخاصة بك بعد الاستخدام عن طريق تقويم الماوس ولوحة المفاتيح والضغط على كرسيك.
- حافظ على كتم صوت الجهاز ما لم تستخدم سماعات الرأس.
- تسجيل الخروج من جميع تطبيقات الويب أو البوابات الإلكترونية عند الانتهاء.
- نظف يديك قبل استخدام الأجهزة وامتنع عن لمسها عندما يتحدث المعلم. لا يسمح بدخول الأطعمة أو المشروبات داخل المختبر.
- تدرب على الكتابة في المنزل لتلبية توقعات المدارس المتوسطة والثانوية وتعزيز تجربتك مع مشاريع التكنولوجيا في مدرسة النخبة العالمية.

توقعات الإنترنت ووسائل الإعلام

- إعطاء الأولوية للسلامة والاحترام والمسؤولية في جميع الأنشطة عبر الإنترنت.
- استخدام الموارد المدرسية للأغراض التعليمية فقط.
- امتنع عن تغيير إعدادات الجهاز.
- لا تلتقط أو تسجل صورا أو مقاطع فيديو للطلاب إلا إذا طلب منك ذلك صراحة.
- قم بالإبلاغ عن أي مشكلات فنية أو مشاكل في المعدات إلى مدرس تكنولوجيا المعلومات والاتصالات على الفور بدلا من محاولة حلها بشكل مستقل.

التركيز على التعلم - وليس تشتيت الانتباه

- يجب استخدام جميع حسابات المدرسة وأجهزتها حصريا للأنشطة المتعلقة بالمدرسة. (لا توجد رسائل أو دردشة لأغراض غير مدرسية).
- ابق على الموضوع أثناء جميع المهام المتعلقة بالمدرسة.
- استخدام الكتابة الصحيحة؛ تجنب الكتابة غير المرغوب فيها أو لغة الرسائل النصية.
- تأكد من أن جميع الصور تعليمية ومناسبة للمدرسة.
- لا تشارك الإجابات على أي تقييمات.

تعهدنا بالمواطنة الرقمية

- سأتواصل بمسؤولية ولطف مع الآخرين.
- سأحترم أفكار وآراء الآخرين.
- سأعطي الفضل المناسب عندما أستخدم عمل الآخرين.
- سأحمي معلوماتي الخاصة ومعلومات الآخرين.
- سأقف في وجه التنمر عبر الإنترنت.
- سأجنب وأبلغ عن أي محتوى ضار أو غير لائق أصادفه عبر الإنترنت.