E-Safety-Cyber Policy 2024-2025

Scope of the Policy

This policy applies to all members of the school (including staff, students, parents, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
To regulate the behavior of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behavior. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

Roles and Responsibilities:

Principal and Senior Leaders:

- Is responsible of reviewing and approving the E-Safety Policy.
- To ensure the safety (including e-safety) of members of the school community
- should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- ensure that there is a system in place, by monitoring and supporting all staff members will be who will take on important monitoring roles.

E-Safety Coordinator:

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety documents
- Ensures that all staff are aware of the procedures that need to be
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents for development
- Review incident logs and filtering / change control logs
- Reports regularly to Senior Leadership Team

Technical staff:

IT support:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack
- The school meets required e-safety technical requirements and any relevant body E-Safety Policy.
- Users can only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- They keep up to date with e-safety technical information in order to effectively carry out their esafety role and to inform and update others as relevant
- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse can be reported to the supervisor / social worker / E-Safety Coordinator / principal.

Teaching Staff:

- To keep awareness of e-safety matters and of the school e-safety policy.
- Must read, and understood and signed the Staff Acceptable Use Policy.
- Should report any misuse or problem to the section supervisor/ social worker for investigation.
- All digital communications with students / parents / should be on a professional level
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Ensure that Students understand the e-safety policy.
- Ensure that Students have a good understanding of research skills and the need to avoid plagiarism
- Must monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities
- implement school policies with regard to these devices.
- Should be aware of the potential for serious child protection / safeguarding issues to arise from:

  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying

Students:

- Have a good understanding of research skills and to avoid plagiarism, and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials
- To understand policies on the use of mobile devices and digital and the use of images and on cyber-bullying.
- Adopting a good e-safety practice when using digital technologies out of school and realize that the Policy covers their actions out of school, if related to their membership of the school.

Parents:

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues providing the necessary information about local e-safety campaigns. Parents will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

• Digital and video images taken at school events

• Access to parents' portal.

EDUCATION Policy Statements

Education – students

The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum.

The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned e-safety curriculum should be provided as part of Computing and other lessons and should be regularly revisited

• Key e-safety messages should be reinforced as part of a planned program of assemblies and activities

• Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

• Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Staff should act as good role models in their use of digital technologies, the internet and mobile devices

• It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Parents

Parents plays an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will provide information and awareness to parents and caregivers through:

• Curriculum activities

• Letters, newsletters, website

• Parents sessions

• events e.g. Safer Internet Day

• Reference to the relevant web sites / publications

Education– Staff /trainees

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A program of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process

• All new staff should receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements

• The E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations

• This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings

• The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure and that policies and procedures are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

• School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements

• There will be regular reviews and audits of the safety and security of school technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices

• The ICT support is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations

• Internet access is filtered for all users

• School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement

• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.

• An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, , visitors) onto the school systems

• Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of Digital Video/ Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents, and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

• When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, they should recognize the risks attached to publishing their own images on the social networking sites

• parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other students / pupils in the digital / video images

• Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

• Students must not take, use, share, publish or distribute images of others without their permission

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images

• Students' full names will not be used anywhere on a website or blog, particularly in association with photographs

• Written permission from parents will be obtained before photographs of students are published on the school website

• Students' work can only be published with the permission of the pupil and parents or carers.

Data Protection (followed as guidelines)

that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Kept no longer than is necessary

• Processed in accordance with the data subject's rights

• Secure

• Only transferred to others with adequate protection.

The school must ensure that:

• It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

• Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

• All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

• It has a Data Protection Policy

• Risk assessments are carried out

• It has clear and understood arrangements for the security, storage and transfer of personal data

• Data subjects have rights of access and there are clear procedures for this to be obtained

• There are clear and understood policies and routines for the deletion and disposal of data

• There is a policy for reporting, logging, managing and recovering from information risk incidents

• There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

• The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access)

• Users must immediately report, to the social worker, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

• Any digital communication between staff and students or parents / caregivers' (email) must be professional in tone and content.

These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications

• Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

• Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the school through limiting access to personal information:

• Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues

• Clear reporting guidance, including responsibilities, procedures and sanctions

• Risk assessment, including legal risk.

School staff should ensure that:

• No reference should be made in social media to pupils, parents / caregivers or school staff

• They do not engage in online discussion on personal matters relating to members of the school community

• Personal opinions should not be attributed to the school

• Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information the school's use of social media for professional purposes will be checked regularly by the e-safety committee to ensure compliance with the social media, Data Protection, Communications, Digital Image and Video Policies.

Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

• Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

• Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following: ➢ Internal response or discipline procedures

➢ Involvement by local organization (as relevant).

➢ Police involvement and/or action

• If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

➢ Incidents of 'grooming' behavior

➢ The sending of obscene materials to a child

➢ Adult material which potentially breaches the Obscene Publications Act

➢ Criminally racist material

➢ Other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with

Policy	E- Safety Cyber policy	Version	**1**
Last Update	August 2024	**Next Update**	August 2025

سياسة السلامة الرقمية - 2024-2025

أهداف العامة للسياسة الرقمية

- هذه السياسة تطبق على جميع أعضاء المجتمع المدرسي بما فيهم: الهيئة التدريسية، الطلبة، أولياء الأمور، الزوار، والمجتمع المحلي؛ أي كل من لديه القدرة على استخدام شبكة الانترنت الخاصة بالمدرسة.
- كما تهدف هذه السياسة لضبط سلوكيات الطلبة أثناء تواجدهم داخل المدرسة وضبط استخدامهم للشبكة العنكبوتية، وتطبيق نظام عقوبات على التصرفات غير اللائقة والمنافية للسياسة الرقمية المطبقة في المدرسة. وهذا يتضمن التنمر الالكتروني وجميع أشكال الجرائم الالكترونية سواء حدثت داخل المدرسة أو خارجها وتسيء للمدرسة أو أحد أعضائها.

الأهداف العامة للسياسة الرقمية

- نشر الوعي و ثقافة الأمن الرقمي.
- تمكين الأهالي والطلبة والمعلمين من مهارات الاستخدام الآمن و الايجابي للانترنت.
- حماية الطفل من مخاطر الانترنت و الجرائم الالكترونية وتوفير بيئة الكترونية آمنة.
- توجيه الطلبة عند رصد سلوكيات ومخالفات رقمية غير مقبولة.
- بناء جيل رقمي يتحمل المسؤولية عند استخدام الشبكة العنكبوتية.

الأدوار والمسؤوليات

أولًا: مديرة المدرسة

- مسؤولة عن الموافقة على سياسة السلامة الرقمية والتأكد من فاعليتها.
- مسؤولة عن ضمان سلامة وأمن جميع أعضاء المجتمع المدرسي- بما يتضمن السلامة الرقمية.
- مسؤولة عن متابعة أي حوادث أو إجراءات تتعلق بانتهاكات ترتكب ضد أعضاء الهيئة التدريسية.
- مسؤولة عن ضمان وجود نظام توجيهي وداعم في المدرسة من أجل تحقيق السلامة الرقمية الداخلية للمدرسة ودعم الذين تولون مهام رئيسية في هذا المجال.

ثانيًا: مسؤول فريق السلامة الرقمية

يرأس لجنة السلامة الرقمية داخل المدرسة ويقوم بمهام يومية تتعلق بالسلامة الرقمية، ومسؤول عن مراجعة الوثائق المتعلقة بها .

- مسؤول عن توفير التدريب المناسب وتوفير النصائح للهيئة التدريسية والإدارية
- مسؤول عن التنسيق والعمل يدا بيد مع فريق الدعم التقني بالمدرسة
- مسؤول عن استلام التقارير الخاصة بحوادث السلامة الرقمية وعمل سجل خاص بها لإجراء التطوير المستقبلي
- مسؤول عن حضور الاجتماعات المتعلقة بمسألة السلامة الرقمية وتقديم التقارير إلى مديرة المدرسة

ثالثًا: فريق الدعم التقني

- مسؤول عن ضمان سلامة البنية الأساسية للشبكة العنكبوتية وأنها غير قابلة للاختراق وسوء الاستخدام.
- مسؤول تحقيق متطلبات السلامة الرقمية
- مسؤول عن ضمان الدخول الآمن للشبكة والأجهزة من خلال تفعيل سياسات أمن وحماية حسابات المستخدمين وكلمات السر، والتي يتم تغييرها بين فترة وأخرى.

- مسؤول عن الاطلاع على التحديثات في مجال السلامة الرقمية داخل المدرسة والتي تمكنه من القيام بواجبه وإعلام الهيئة التدريسية بهذه المستجدات.
- مسؤول عن مراقبة الشبكة والتعلم عن بعد وحرية الوصول إليها وأمن البريد الالكتروني وارسال التقارير الى المشرفين والأخصائية الاجتماعية والمديرة ومنسق السلامة الرقمية

رابعًا: الهيئة التدريسية

- عضو الهيئة التدريسية مسؤول عن الاطلاع على المستجدات الخاصة بسياسة السلامة الرقمية في المدرسة.
- عضو الهيئة التدريسية مسؤول عن قراءة، وفهم، وتوقيع وثيقة سياسة الاستخدام المقبول للانترنت في المدرسة.
- عضو الهيئة التدريسية مسؤول عن ربط السلامة الرقمية وتضمينها في المنهج والنشاطات التعليمية.
- عضو الهيئة التدريسية مسؤول عن التبليغ عن أي سوء استخدام أو مشاكل إلى الأخصائي الاجتماعي ومسؤول القسم.
- عضو الهيئة التدريسية مسؤول عن توعية الطلبة عن سياسة السلامة الرقمية.
- عضو الهيئة التدريسية مسؤول عن ضمان فهم الطلبة لمهارات البحث والاستقصاء وضرورة تجنب انتهاك حقوق الملكية الأدبية.
- عضو الهيئة التدريسية مسؤول عن التحكم في استعمال التكنولوجيا الرقمية وأجهزة الهواتف النقالة والكاميرات في الدروس والأنشطة المدرسية واستخدامها ضمن سياسة الاستخدام المقبول للتكنولوجيا في المدرسة.
- عضو الهيئة التدريسية يجب أن يكون ملمابقوانين حماية الطفل والحفاظ على أمنه.

خامسًا: الطلبة

- فهم مهارات البحث والحاجة إلى تجنب انتهاك الملكية الأدبية للغير
- فهم أهمية التبليغ عن الانتهاك وسوء الاستخدام للتقنيات الرقمية والدخول إلى أي محتوى غير ملائم أو مواقع محظورة ومعرفة كيفية الإبلاغ عن مثل هذه الحوادث.
- يتوقع منه فهم واستيعاب سياسة استخدام الأجهزة الذكية
- يدرك أهمية تبني ممارسات صحيحة للاستخدام الرقمي عند استخدام التقنيات الحديثة خارج المدرسة وإدراك ان سياسة السلامة الرقمية للمدرسة تشمل جميع أفعالهم خارج المدرسة التي تتعلق بالمجتمع المدرسي

سادسًا: أولياء الأمور

- يلعب أولياء الأمور دورا هاما في ضمان وتأكيد فهم حاجة أبنائهم الى استخدام الانترنت والشبكة الذكية بطريقة سليمة ومقبولة، وتقوم المدرسة بمساعدة أولياء أمور الطلبة بفهم هذه السياسات من خلال عقد اجتماعات وورشات عمل ونشر الرسائل التوعوية التي تتعلق بالسلامة الرقمية.

- تقوم المدرسة بتعزيز دور أولياء الأمور في المساهمة في رفع الوعي حول السلامة الرقمية وذلك باستخدام الدليل الإرشادي في الطريقة الصحيحة لاستخدام الصور والمقاطع الرقمية التي يتم نشرها من خلال المدرسة، وتسهيل الوصول إلى بوابة أولياء الأمور المدرسية

مبادئ توجيهية لسياسة التعامل مع التنمر الإلكتروني

التنمر الإلكتروني : وهو تنمر باستخدام التقنيات الرقمية ،ويمكن أن يحدث على وسائل التواصل الاجتماعي ومنصات المراسلة ومنصات الألعاب والهواتف المحمولة ، وهو سلوك متكرر يهدف إلى إخافة أواستفزاز المستهدفين به أو تشويه سمعتهم .

- المضايقة عن طريق الإرسال المتكرر لرسائل نصية أو لرسائل فورية في غرف المحادثة تؤثر سلبياً على الشخص الذي تعرض له ؛ لهذا تتم وضع بعض المبادئ التوجيهية لسياسة التعامل مع التنمر الإلكتروني و ذلك لمواجهته و لضمان سلامة طلبتنا في المدرسة.

1- تمنع المدرسة القيام بأي تصرف يخل بالسلوك و النظام في المدرسة بما فيه أي نوع من التنمر أو التنمر الإلكتروني.

2- تنشر المدرسة لائحة إدارة سلوك الطلبة لجميع عناصر المجتمع المدرسي .

3- تنفذ المدرسة برامج توعوية حول الاستخدام الآمن والاستخدام غير المقبول.

4- يقوم فريق السلامة الرقمية بمراقبة المخالفات الالكترونية والتي يمكن أن تصدر عن المجتمع المدرسي .

5- يقوم فريق السلامة الرقمية في المدرسة بالتعامل مع أي حالة تنمر إلكتروني وفق لائحة إدارة السلوك

6- في حال قام الطالب الإبلاغ نيابة عن أحد أصدقائه في حالة تعرضه للتنمر الإلكتروني و على المدرسة التحقق من ذلك .

.7- يجب على الطالب الحفاظ على الأدلة التي تثبت التنمر مثل رسائل البريد الإلكتروني أو الرسائل النصية المزعجة و غيرها فهذا سيساعد في كشف هوية المتنمر

سياسة السلامة على الانترنت

حرصا على سلامة الطالب ولتوفير بيئة مناسبة آمنة للتعليم تلتزم المدرسة الوطنية بتطبيق نظام شامل ومتكامل للدعم الالكتروني وحماية الطلاب.

أسس لنظام بمشاركة الهيئات الادارية والتعليمية من اجل العمل على توعية وتثقيف الكوادر التعلبمبة واشراك الاهالي مع الطلبة.

تقع مسوؤلية متابعة الطلبة الكترونيا ورصد مشاكلهم على المدرسة بالاضافة الى ايجاد الحلول المناسبة لهذه المشاكل.

تم وضع السياسة بدقة بالاستناد الى الموجهات التالية :

1- الاستراتيجية الوطنية للأمن السيبيراني.

2-قانون حماية الطفل(وديمة).

3- سياسة المشاركة الرقمية لوزارة التربية والتعلبم .

4.دليل الاجراءات والتبليغ لوحدة حماية الطفل.

5.لائحة ادارة سلوك الطلبة في التعلم عن بعد.

سياسة استخدام أجهزة التعلم الذكي

- 1- الجهاز يستخدم للأغراض التعليمية فقط أثناء ساعات الدوام الرسمي.
- 2- عدم كتابة أو نشر تعليقات مسيئة أو غير لائقة فيما يتعلق بالطلبة أو المعلمين أو المدرسة و إلحاق الضرر بهم على وسائل تقنيات المعلومات المختلفة.
- 3- أن يلتزم الطالب بلائحة السلوك المدرسية.

إدارة التقنيات الرقمية

الكوادر التعليمية و الموظفين:

- تفعيل حسابات خاصة للموظفين مع متابعة المشاكل والصعوبات.

- تثقيف الموظفين بالطرق الصحيحة لتأمين وحماية الحسابات و التبليغ في حالة الاختراق للحسابات

الأهالي:

- التواصل المستمر مع المدرسة عبر قنوات التواصل الخاصة بالمدرسة.

- الاطلاع على لائحة سلوك الطلبة في التعلم عن بعد و توجيه ابنائهم للالتزام بها.

- الابلاغ في حالة المشاكل او المخالفات و الاختراقات عبر الخط الساخن او قنوات التواصل الخاصة بالمدرسة.

- التوجيه و الارشاد للابناء نحو الاستخدام الايجابي للشبكة.

- متابعة اي تحديثات بالبروتوكولات والقوانين.

الطلبة:

- الالتزام بالقوانين والتوجيهات الصادرة من الوزارة.
- الالتزام باستخدام المنصات الوزارية المعتمدة.
- الابلاغ عن أي مخالفة او انتهاك للخصوصية.

دور فريق السلامة الرقمية

متابعة المحتوى المتعلق بالمدرسة وما يتم نشره عنها من قبل المستخدمين

التأكد من سلامة الروابط التي يتم نشرها

المساعدة في حل المشكلات التقنية

موا صفات المواطن الرقمي

- يدير الوقت الذي يقضيه في الانترنت
- يلتزم بالأمانة الفكرية
- يحمي نفسه من المعتقدات الفاسدة التي تنشر عبر الوسائط
- يقف ضد التسلط عبر الإنترنت
- يحترم الثقافات والمجتمعات في البيئة الافتراضية
- يحافظ على المعلومات الشخصية

التعليم

الطلاب: توعية الطالب بأهمية كونه مسؤول عن استخدامه للأجهزة الذكية وتقوم المدرسة بدعم الطلاب وتوعيهم ضد مخاطر الأجهزة الذكية وبناء القدرة لديهم على التعامل مع الحالات والمخاطر التي تواجههم

يتم التركيز على السلامة الرقمية من خلال المنهج وإرسال رسائل تدعم هذه السلامة عبر المنهاج لضمان فهم الطلاب وادراكهم لمفهوم السلامة الرقمية ويتم ذلك من خلال عمل نشاطات إبداعية تقدم بالطرق التالية:

- دعم السلامة الرقمية من خلال برامج الإذاعة المدرسية
- توعية الطلبة على أهمية المحتوى الرقمي الذي يستخدمونه والانتباه الى صحة ودقة المعلومات المستخرجة
- أتشكل الهيئة الادارسة والتعليمية نموذجا من خلال استعمالهم للتقنيات الرقمية، الانترنت او الأجهزة المتنقلة

أولياء الأمور: يلعب أولياء الأمور عنصرا هاما في تعليم أبنائهم السلامة الرقمية وارشادهم الى السلوك الصحيح وقد يكون لديهم عدم ادراك وتقليل لأهمية دخول الطالب الى مواقع محظورة على الانترنت ولا يوجد عندهم وعي لكيفية التعامل مع مثل هذه الحالات, لذلك تقوم المدرسة بتقديم الدعم والوعي لأولياء الأمور من خلال:

- النشاطات المنهجية
- وسائل لنشر التوعية على مواقع التواصل
- ورشات عمل لأولياء الأمور
- الاحداث والمناسبات مثل يوم السلامة الرقمي

الهيئة التعليمية: تحرص المدرسة الوطنية على أن يتلقى أعضاء الهيئة التدريسية التدريب ليتمكنوا من فهم ادوارهم من خلال هذه السياسة ويمكن تقديم هذا التدريب عن طريق:

-عقد ورشات تعليمية خاصة بالسلامة الرقمية

- حضور الموظفين الجدد ورشات عمل مدرسية تمكنهم من فهم السياسة العامة للمدرسة والسياسة المقبولة لاستخدام اجهزة التقنيات الرقمية

-عمل تحديثات دورية للسياسة بين فترة والأخرى

- حضور ورشات خارجية تتعلق بالسلامة الرقمية

- تقديم النضج والإرشاد والتدريب من خلال منسق السلامة الرقمية الموجود بالمدرسة

البنية التحتية

تحرص المدرسة على وجود أنظمة فعالة لضمان امان أنظمة الكمبيوتر بالمدرسة ومستخدمي النظام والبيانات السطحية كما انه على المدرسة إدارة النظام التقني لديها بما يناسب احتياجاتها الاكاديمية على ان تكون هناك مراجعات دورية وتعديلات للنظام التقني للمدرسة حسب الاحتياجات كما أنها تملك القدرة على إدارة الوصول الى المحتويات الموجودة على أنظمتها وتقوم بإدارة النشاطات التي تتم عليها لحماية المستخدمين والابلاغ عن الحوادث والتعامل معها.

تراعي المدرسة الوطنية الحاجة الى ممارسات تلائم المرحلة العمرية للمستخدمين بالإضافة الى حاجة المدرسة الى استخدام سجلات لكلمات المرور وآليات استعادتها وتغييرها.

استخدام التقنيات الرقمية

تلعب هذه دورا هاما في العملية التعليمية كما لها اثر على الطلاب لذلك تحرص المدرسة الوطنية على ان يكون الطلاب والهيئة التدريسية واولياء الأمور على وعي تام بمخاطر نشر الصور والفيديوهات على الانترنت لأنه قد يكون هناك عرضة للتنمر الالكتروني

تقوم المدرسة الوطنية بتوعية المستخدمين حول هذه المخاطر وتطبيق السياسات التي من شأنها حد المخاطر

- لا مانع لدى المدرسة ان يقوم أولياء الأمور بالتصوير والتقاط صور لأبنائهم اثناء تواجدهم في المدرسة مع ضمان عدم مشاركتها او نشرها الا بما يتناسب مع سياسة المدرسة

- يسمح للهيئة التدريسية بالتقاط مقاطع الفيديوهات وللصور لدعم اهداف تعليمية مع اتباع سياسة المدرسة فيما يخص نشر هذه الوسائط

- يجب الحصول على اذن ولي الامر قبل التقاط الصور ونشرها على مواقع التواصل الاجتماعي

وسائل التواصل

يمكن لوسائل التكنولوجيا أن تطور التعليم وتسهّل وسائله مع الأخذ بعين الاعتبار:

- يقوم المستخدمون بالتبليغ عن أي وسيلة تواصل تشعرهم بعدم الأمان والراحة، مهينة، مهددة أو تنمر الكتروني إلى الجهات المختصة وعدم الاستجابة أو الرد على هذه الوسائل.

- أي تواصل رقمي بين الهيئة التدريسية والطلاب أو أولياء الأمور يكون رسميا

- تقوم المدرسة بعمل جلسات توعية للطلاب ويتم تعليمهم عن أهمية السلامة الرقمية, مثل مخاطر مشاركة المعلومات الشخصية. ويجب عليهم معرفة استراتيجيات التعامل مع أي وسيلة تواصل تشعرهم بعدم الأمان والراحة وأن يعلموا كيفية استخدام مواقع التواصل بأمان وبطريقة فعالة

سياسة الاستخدام المقبول

- يمنع تحميل البرامج التجارية والمحمية بحقوق الطبع والنشر بدون ترخيص رسمي
- تقوم المدرسة بمراقبة المنصات التعليمية وتحركات الطلبة ورصد أنشطتهم بانتظام
- يقوم أعضاء المجتمع المدرسي باستخدام المراسلات والقنوات الرسمية لاستخدام العمل فقط وليس للمصالح الشخصية وعدم فتح المراسلات غير معروفة المصدر.

- يجب أن يكون محتوى الأنشطة التي يقدمه الموظف موافقا لسياسات وزارة التربية والتعليم
- يجب على الموظف التخلص السليم من المراسلات السرية وعدم نشرها في مواقع التواصل الاجتماعي

سياسة الاستخدام المقبول لأولياء الأمور

- تعمل المدرسة على توعية أولياء الأمور حول محافظة أبنائهم على الأجهزة الوزارية من أي تلف أو تحميل برامج أو ألعاب يعرضها للفيروسات وغيره
- توعية أولياء الأمور ابناءهم ومراقبتهم لرصد حوادث التنمر والابلاغ عنها واتباع لائحة السلوك وعدم التهاون بها
- التواصل الدائم مع المدرسة بما يصب في مصلحة الطالب في حالة وجود شكوى / ملاحظة أو استفسار

اطلاع أولياء الأمور على سياسات استخدام التقنيات

- تعمل المدرسة على توعية أولياء الأمور حول محافظة أبنائهم على الأجهزة الوزارية من أي تلف أو تحميل برامج أو ألعاب يعرضها للفيروسات وغيره
- توعية أولياء الأمور ابناءهم ومراقبتهم لرصد حوادث التنمر والابلاغ عنها واتباع لائحة السلوك وعدم التهاون بها
- التواصل الدائم مع المدرسة بما يصب في مصلحة الطالب في حالة وجود شكوى / ملاحظة أو استفسار
- اطلاع أولياء الأمور على سياسات استخدام التقنيات الرقمية

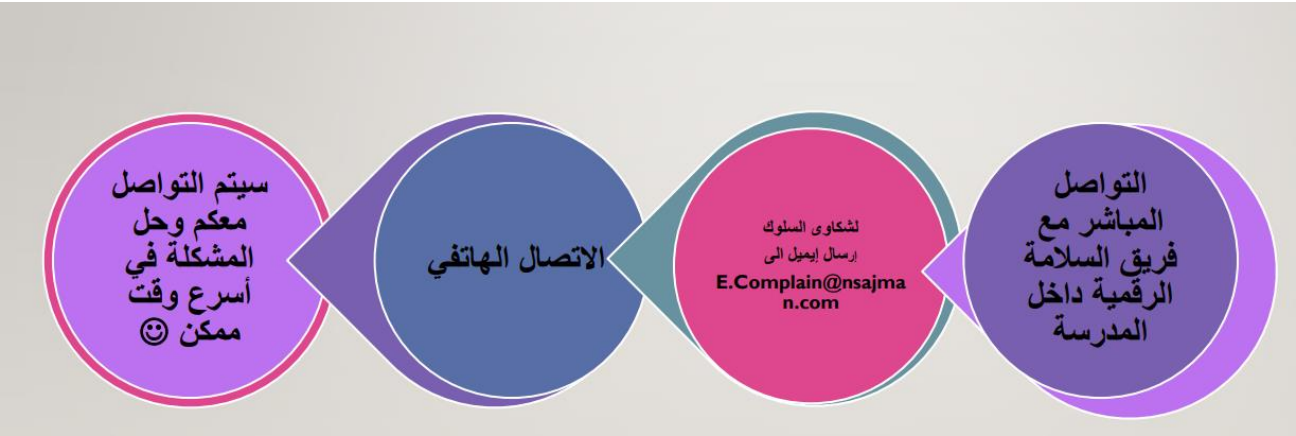
سياسةالاستخدام غير المقبول

- استخدام لغة أو ألفاظ غير مناسبة.
- استقبال أو ارسال أي مواد فاحشة أو إباحية.
- مواد فاحشة أو إباحية.
- اعطاء معلومات شخصية مثل العنوان أو رقم التليفون أو أسماء أفراد الأسرة، أو ترتيب موعد مع شخص تعرفت عليه من خلال الإنترنت.
- إرسال رسائل تتعلق أو تدعم الأنشطة غير القانونية مثل بيع أو استخدام المخدرات أو الكحوليات، أو دعم الأنشطة الإجرامية أو أنشطة العصابات أو التهديدات أو الترويع أو التحرش بأي شخص.
- استخدام الأنترنت على نحو عرقلة استخدام الآخرين مثل نشر فيروسات أو إرسال رسائل مسلسلة.
- تنزيل مواد لها حقوق نشر بدون إذن المالك.
- استخدام البريد الإلكتروني لأي شخص آخر أو كلمة المرور الخاصة به.
- الاشتراك في قائمة خدمات أو مجموعات الأخبار أو إرسال الايميلات إليها بدون إذن من المدرسة.

آلية الإبلاغ

عزيزي الطالب:

- ✓ اتبع آلية التبليغ حتى نساعدك في حل المشكلة.
- ✓ احرص على اتخاذ الإجراءات الصحيحة في الإبلاغ عن المشكلة حتى تُحفظ حقوقك.
- ✓ أرسل البيانات الصحيحة عبر البريد الإلكتروني كي نحل المشكلة في وقت أقصر.
- ✓ سيتم التواصل معك من قبل فريق السلامة الرقمية وتقديم حلول أولية إلى حين حل المشكلة تمامًا.



تفاصيل السياسة	سياسة السلامة الرقمية		
أخر تحديث للسياسة	أغسطس 2024	التحديث القادم	أغسطس 2025