E-Safety Policy

CONTENTS

In an age where technology is an integral part of education, our school recognizes the need to provide a safe and secure digital environment for our students. This E-Safety Policy has been developed to outline our commitment to the responsible and ethical use of digital technologies within the school community.

1. Purpose:

The primary purpose of this policy is to safeguard our students from potential online risks and empower them to navigate the digital world responsibly. By establishing guidelines for the use of digital devices and online platforms, we aim to foster a culture of digital citizenship that aligns with our commitment to providing a nurturing and protective learning environment.

2. Scope:

This policy applies to all students, teachers, staff, and any other individuals associated with our school who engage with digital technologies within the school context. It encompasses the use of school-provided devices, networks, and any online platforms used for educational purposes.

3. Importance of E-Safety in Education:

As technology continues to play a pivotal role in education, it is imperative to balance the benefits of digital tools with a commitment to online safety. Our e-safety policy is designed to equip students with the knowledge and skills needed to navigate the online world responsibly, promoting a positive and secure learning environment.

4. Key Principles:

Our e-safety policy is built on the following key principles:

- Protection of students from online risks, including cyberbullying and inappropriate content.
- Promotion of responsible and ethical use of digital technologies.
- Integration of e-safety education into the curriculum to enhance digital literacy.

- Collaboration with parents, teachers, and students to create a holistic approach to online safety. We recognize that ensuring e-safety is a joint effort involving parents, teachers, and the wider school community. Our school is committed to working collaboratively to educate, support, and guide students in the responsible use of technology both at school and at home.

5. Continuous Review and Improvement:

In acknowledgment of the evolving nature of technology, this e-safety policy is being regularly reviewed and updated. This ensures that it remains relevant, effective, and aligned with the ever-changing landscape of digital technologies. By embracing the principles outlined in this e-safety policy, our school aims to provide a secure and empowering digital learning environment that prepares students to thrive in the 21st century while prioritizing their safety and well-being.

6. The aims of an e-safety policy:

The aims of an e-safety policy typically include:

- **Protecting Users:** The primary aim is to safeguard the well-being of users, such as students, employees, or any individuals associated with the organization, from potential online risks and threats. This includes protection from cyberbullying, inappropriate content, and online predators.
- **Promoting Responsible Use:** Encouraging responsible behavior online is a key objective. This involves educating users about the appropriate use of digital technologies, respecting others' privacy, and understanding the consequences of online actions.
- **Preventing Cyberbullying:** E-safety policies often address cyberbullying specifically, outlining measures to prevent and respond to instances of online harassment or bullying. This includes educating users on recognizing and reporting such incidents.

- **Managing Personal Information:** Ensuring the secure handling of personal information is crucial. The policy should provide guidelines on how to protect and manage personal data, including guidelines on privacy settings and data sharing.

- **Compliance with Laws and Regulations:** The policy aims to ensure compliance with relevant laws and regulations related to online safety data protection. This may include adherence to national or regional data protection laws, as well as regulations specific to the organization's sector.
- **Providing Guidance and Education:** Offering educational resources and training to users is essential. This includes providing information on online safety practices, awareness campaigns, and training sessions to enhance digital literacy and cybersecurity awareness.
- **Implementing Technical Measures:** The policy may outline technical measures to be implemented, such as firewalls, content filters, and other security tools, to protect users and the organization's network from potential threats.
- **Establishing Reporting Procedures:** Clear reporting procedures for incidents or concerns related to online safety should be established. Users should know how to report inappropriate content, cyberbullying, or any other online safety issues.
- **Collaboration with Parents/Guardians:** E-safety policies often include provisions for involving parents or guardians in the education process. This may include providing resources for parents to understand and support their children in safe online practices.
- **Regular Review and Updating:** The policy should be a dynamic document that is regularly reviewed and updated to reflect changes in technology, emerging threats, and evolving best practices in online safety.

7. Acceptable use of Technologies for students:

The technology usage policy at Al Rushed American private school explains the rules that must be followed when using computers, the network, e-mail, and internet services in accordance with the regulations and policies set by the state, the Sharjah authority for private education and the school to enhance digital security in the school environment. these are some of the laws that determine the Acceptable Use of technologies in school:

● The school allows the student to bring his mobile device (computer or tablet) to school when needed according to the specifications determined by the school with the pledge to use it for educational purposes only.
● The school provides the student with access to platforms related to the educational process that promote the acquisition of knowledge and help him perform his duties.
● Users should contribute and participate in information security activities organized by the school (such as awareness in the field of cyber security).
● Student users are responsible for the appropriate use and dissemination of information through the e-mail services provided by the school.
● Awareness of not posting socially and morally inappropriate comments, whether a private photo, an article or a video posted on the internet.
Awareness of not posting electronic posts, rumors or information with the aim of offending or discrediting another person or the school.
● Awareness of not doing anything that violates the behavior and regulations of the school system, including any form of cyberbullying, and the school will take strict and disciplinary measures to maintain a safe and disciplined atmosphere in the school.
● The school has the right to monitor and monitor every activity carried out by the student on educational platforms and websites.
● The school provides secure internet access to all students by providing approved protection programs.

8. Unacceptable use of technologies for students:

The technology usage policy at Al-Rushed American private school explains the rules that must be followed when using computers, the network, e-mail, and internet services in accordance with the regulations and policies set by the state, the Sharjah authority for private education and the school to enhance digital security in the school environment. these are some of the laws that determine the unacceptable use of technologies in school:

● It is prohibited to use the internet to send, download or publish any offensive or immoral material that violates the laws, rules, and regulations in force in the country.

● It is forbidden to photograph or record teachers or students and post photos or recordings on various media.

● Do not impersonate other characters or use the personal account of another student.

● The student is not allowed, intentionally or unintentionally, to download any program that destroys computer files, confuses users, or obstructs the performance of the hardware system.

● Awareness of not doing anything that violates the behavior and regulations of the school system, including any form of cyberbullying, and the school will take strict and disciplinary measures to maintain a safe and disciplined atmosphere in the school.

● It is prohibited to publish any ideas that would incite hatred, racism, or disturb public order or morals.

● It is forbidden to promote any commercial product or call for fundraising.

● It is forbidden to download commercial software, or any materials protected by copyright and intellectual property without a license.

● The student is not allowed to bring a mobile phone, smart watches, and cameras to school except for the device specified by the school and the school is not responsible for any device damaged or lost at school.

● It is forbidden to download/ upload any programs, games, or videos etc.

● The school has the right to monitor and monitor every activity carried out by the student on educational platforms and websites.

9. Acceptable use of Technologies for the administrative and teaching staff:

The school provides the teacher and the employee with access to the internet to help them carry out their assigned tasks, whether related to the educational process or correspondence, and it is not used for other purposes unrelated to work. The teacher bears the responsibility for using the internet. The school also has the right to monitor and monitor every activity carried out by the teacher on educational platforms and websites only.

- The school provides e-mail, username, and PIN number for each employee with the need to change his PIN number periodically.
- Awareness of the non-exchange of work username and password between employees.
- Indicate the source of digital content when making use of it and do not copy copyrighted materials.
- Advocacy, promotion of any commercial product or fundraising is allowed only with a license approved by the competent authority.
- Awareness of not using any accounts or saving personal data on the school device.
- Caution when using unsafe data savers or DVDs.
- It is allowed to download videos from the internet that will be shown to students if they do not contradict the school's policies.
- It is acceptable to participate in all activities that contribute to the strengthening and improvement of the professional side of the employee, including online research and training.
- The school provides the teacher with programs to monitor students to ensure that they do not visit any unauthorized website.
- It is allowed to download and upload any programs to the school device after the approval of the relevant department (Digital Safety Officer).
- Allows the use of the school's e-mail for work purposes.

● Allows the use of all available online teaching resources in teaching and learning activities that involve research and cooperation with the rest of the staff in the educational field.

● Teachers employ technology in New and innovative ways to stimulate student learning and Twenty-First Century Skills Development.

● Provide accurate digital content relevant to various educational fields.

● Checking the accuracy and correctness of information and evaluating various sources on the internet.

It allows contributing to raising students ' awareness of the importance of technology and how to use it to make the most of it.

● Raising students ' awareness of their rights and responsibilities and using digital technology responsibly, awareness and adherence to the Acceptable Use Policies by the competent authorities, digital laws and ethical regulations set by the school.

● It is allowed to publish photos or videos of students on various websites, but after consulting the school administration.

● The teacher using the school network should contact the school's complaints department when noticing any security problem and report Risks, security violations, and any illegal material or content.

10. Unacceptable use of technologies for the administrative and teaching staff:

● Not to mention the reference to the source of digital content when making use of it and not to copy copyrighted materials.

● Hacking and disrupting the network or unauthorized access to data or accounts without official permission is prohibited.

It is prohibited to send confidential data or information about the school or employees to any party outside the employer that could harm or defame the reputation of the school.

● It is prohibited to invite, promote any commercial product or collect donations without an authorized license from the competent authority.

Awareness not to send, upload or publish any material that incites sedition, hatred, racism or sectarianism, harm national unity or social peace, or disturb public order or public morals.

- Caution when using unsafe data savers or DVDs.
- It is forbidden to download videos that will be shown to students on scenes that contradict the school's policies.
- The teacher should monitor the students to ensure that they do not visit any website that is not allowed.
- It is forbidden to download and upload any programs to the school device that impede the performance of the system.
- Do not use your work email for personal purposes.
- The accuracy and correctness of the information should be checked and evaluated by various sources on the internet.
- It is forbidden to publish photos or videos of students on various websites unless they refer to the school administration.

11. Acceptable use of Technologies for parents:

The school's Acceptable Use Policy explains the rules that must be followed when using computers, network, e-mail, and internet services in accordance with the regulations and policies set by the state, the Sharjah authority for private education and the school to enhance digital security in the school environment and the school encourages everyone to take responsibility when using safe technology:

- The Guardian has the right to access the web at the expense of the Wi-Fi (Guest) only.
- The parent is allowed to use the websites for purposes that do not contradict the school's policies.
- The parent is allowed to communicate with the school through the available communication channels, provided that the communication is decent and does not contradict the laws and regulations followed in the country.

- It is allowed to copy and publish photos and videos electronically after the approval of the administration at the school.
- Allows the parent using the school network to communicate with the school's complaints department when noticing any security problem and immediately report security risks and violations.
- It is allowed to use the computer provided by the school inside the building in a designated place for surfing the internet.
- Instructing children to maintain the confidentiality of passwords for e-mail and educational school systems such as the Tims platform.
- The parent must report the existence of any misuse of the school's platforms or the existence of any defect in his own powers regarding the use of these platforms.

12. Unacceptable use of technologies of parents:

The unacceptable use policy at the school explains the rules that must be followed when using computers, the network, e-mail, and internet services in accordance with the regulations and policies set by the state, the Sharjah authority for private education and the school to enhance digital security in the school environment and the school encourages everyone to take responsibility for their safe use of technology:

- When using the school's wireless (Wi-Fi) connection, the parent has the right to access the web only through the (Guest) account.

- It is forbidden to use the internet to send, download or publish any offensive or inappropriate material that violates the laws, rules, and regulations in force in the country and at school, or contrary to morals or Islamic teachings.

- It is forbidden to shoot or record without prior permission from the administration.

- It is forbidden to use social media to write or post offensive or inappropriate comments related to the school community.

● Access to suspicious sites is not allowed to hack or download programs that affect school devices, such as spreading viruses or sending messages that hinder or damage the functioning of devices.

● It is prohibited to carry out any behavior that violates behavior and order in the school, including any kind of bullying or cyberbullying, and the school will take the legal procedures followed in the country.

● It is forbidden to download commercial programs, or any materials protected by copyright and intellectual property without a license.

● The parent should not be secretive when noticing any security problem when using the internet and report it immediately.

The school has the right to take the measures it deems appropriate in accordance with the regulations and laws followed by the Sharjah authority for special education and the school against those who violate these policies.

13. Roles and Responsibilities:

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

a. Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Coordinator
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / Committee / meeting

b. Principal and Senior Leaders:

- The principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The principal and (at least) another member of the Senior Leadership Team 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
- The Principal and Senior Leaders are 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
- The principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

c. 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 policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the SPEA / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

d. IT Coordinator / Technical staff:

The IT Coordinator & IT Technician are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any SPEA / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with e-safety technical information in order to effectively carry out their e- safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Year / Principal / Senior Leader; E-Safety Coordinator.

e. Teaching and Support Staff

Are responsible to ensure that

- They have an up-to-date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement
- They report any suspected misuse or problem to the Head of Year for investigation / action / sanction
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems

- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies about these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

f. Child Protection / Safeguarding Lead

Should be trained in e-safety issues and 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

g. Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- Will be expected to know and understand policies on the use of mobile devices and digital cameras.

They should also know and understand policies on the taking / use of images and on cyber-bullying.

- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

h. 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 through parents' evenings, newsletters, letters, websites, and information about national / local e-safety campaigns / literature. Parents and caregivers 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' sections of the website / blog
- Their children's personal devices in the school (where this is allowed)

i. Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User before being provided with access to school systems.

Policy Review

Created: June 2022

Reviewed: Jan. 2024