E-SAFETY POLICY

2025-2026

AIMS OF THESE GUIDELINES

The safeguarding of students is always of prime concern to the school and is an equally important issue in the virtual online world as it is in the physical. Issues with the online safety of students increase as technology develops and, therefore, policies and practices must be in place to grow with the changing risks that students face.

The guidelines below set out to provide directions for supporting all students at the Al Resalah International School of Science (RISS) in their online endeavors. These guidelines lay out the purpose of the Online Safety Group and the actions it should take to ensure all students are safe when using the virtual world for school purposes. Training and support are also something that the group will oversee to ensure that all staff, students and parents have an increasing awareness of online safety whenever they are using technology, for both school and personal purposes.

The Al Resalah International School of Science ensures that:

- Students can safely access new technology and learn how to participate in the digital world without compromising their safety and security.
- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- All students and staff understand the importance of password security and the need to log Out of accounts.
- Staff act as good role models in their use of ICT, the Internet, and mobile devices
- It has a clear and understood arrangement for the security, storage, and transfer of personal data.

- To create awareness among the stakeholders on 'the various initiatives of U A E concerning child protection by incorporating **Federal Law No: 3 of 2016 (Wadeema's Law)- Federal Law No. 3 of 2016** concerning child rights, which states that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services facilities without any kind of discrimination, **Federal Law No: 5 of 2012 on combatting cybercrimes –** the article of this law highlights several computer and online related activities and how they would be dealt with under the law. It addresses subjects such as IT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more. etc.
- It will deal with incidents within this policy and associated behavior and anti-bullying

policies and will, where known, inform parents/caregivers of incidents of inappropriate e-safety behavior that take place outside of school.

Rationale

Technology has arrived to stay. Its impact on education has been profound and this has increased many folds ever since the pandemic of 2020. Overnight all of education moved into online mode without much prior knowledge and unaware of the perils. And there is no denying that the changes that education has seen over the last year is here to stay.
However, over the months that have passed, the understanding of online technology has improved and the realization that this requires a strong footing in safety and security has also become evident. In such a situation it becomes imperative to have a strong online safety policy that gives a clear picture of what is expected. It is also essential to connect this policy to other policies of the school to make it integral.

The Online Safety Policy of RISS School aims to do ensure the safe use of digital resources and technology.

Scope

This policy applies to all members of the school (including staff, students, parents, and visitors) who will have access to and are users of school digital systems, on-campus and/or remotely.

Review

Due to the ever-changing nature of digital technologies, the school shall review the Online Safety Policy quarterly and, if necessary, at other instances in response to any significant new developments in the use of the technologies, new threats to online safety, local regulations, or incidents that may take place.

Roles and Responsibilities

The designated Online Safety Leader shall take responsibility for any online safety issues and concerns and will be leading the online safety group. There are certain roles and responsibilities laid down to ensure the implementation of this Policy.

RESPONSIBILITIES OF THE MEMBERS OF THE ONLINE SAFETY GROUP

Whole-Group Responsibilities:

- Develop, Monitor, and review all e-safety, online, and relevant IT policies and procedures
- Monitor the online e-safety incident record (managed by the Student Wellbeing Team)
- Be made aware of any incidents that may occur and work with the Student Wellbeing Team to help decide on any actions required where necessary
- Monitor any issues that may arise and be up to date with changes and developments in technology that may, in particular, have an impact on student safeguarding (e.g. new apps, changes in security permissions)
- Discuss and decide on training and awareness programs for various members of the school community, develop and deliver the programs, and review them through feedback from the participants
- Oversee the development of an ongoing broad e-safety curriculum, its development, implementation, and review of its effectiveness
- Oversee all activities and programs offered to promote e-safety

Roles and Responsibilities of Online Safety Leader

- Provide leadership to the e-safety initiative of the school.

- Develop an e-safety culture in the school through a varied range of initiatives such as events, training, workshops, curriculum, and so on.
- Receive necessary training in e-safety, child protection, and related topics and keep updated about the latest developments on the same.
- Ensure that all members of the online safety group know their responsibilities and carry them out diligently.
- Have scheduled meetings with the group to discuss and address the e-safety needs of the school.
- Convene emergency meetings in case of any incidents that require immediate attention and action.
- Ensure that all meetings have proper minting and the same is filed for future reference.

See to it that all departments systematically document all required matters related to e-safety such that they are easily accessible.

- Work with the school management, Principal, and HR Department to understand, develop, and impart continuous training to the staff on online safety, acceptable use, child safety, anti-bullying, and all matters related to e-safety.
- Ensure that e-safety policies are properly executed, reviewed, and updated.
- See the embedding of e-safety threads across policies of the school where they are relevant and essential.
- Develop, implement, and monitor reporting strategies and systems to ensure that all e-safety safety incidents happening in and beyond school are addressed and followed up properly.
- Ensure that the e-safety curriculum is developed, imparted, and updated as per plans.
- Work with the school team to plan and execute events and activities throughout every school year to promote e-safety.
- Follow up and receive appropriate MIS to ensure that all scheduled audits and monitoring of e-safety infrastructure are on track.
- Ensure that parents are informed and involved in the e-safety journey of the school.

- Liaise with government and non-government agencies to stay updated and also report any incidents that require outside-the-school intervention/advice.
- Understand the statutory requirements of e-safety in UAE and ensure that the school systems comply.
- Generate reports for the school management and/or leadership concerning e-safety every 6 months and as per the demand.
- Represent the school for seminars and meetings on e-safety.
- Do adequate research, and connect with various organizations and communities so that all the latest development in e-safety is known, and the same is integrated into the school where relevant.

Roles and Responsibilities of Online Safety Assistant Coordinator (Staff representative)

- Work closely with the online safety leader in leading the committee and all roles and responsibilities.
- Follow up on the plans for the year and ensure that they are being carried out systematically.
- Advise the online safety leader of any deviations from plans or any breaches that need attention from the leader and the group. Guide the Student Online Safety Group in their activities.

Roles and Responsibilities of Child Protection Officer (School Counsellor)

- Take the lead along with the online safety leader in ensuring child protection.
- Immediately respond or step in when an online child safety incident occurs and work with the online
- Safety leader, parents, and students as required to address the same.
- Ensure that the evidence of intervention is documented.
- If appropriate, advise Online Safety Leader and school leadership for referral to external agencies.
- Be a part of the development, implementation, and review of the child protection policies of the school.

- Actively participate in the development of training modules for stakeholders on child protection, online behaviors, and anti-bullying.
- Obtain training on handling various child protection and e-safety issues and stay updated on the same.

Roles and Responsibilities of Parent Representatives

- Assist the school in ensuring widespread parent participation in workshops and events of the school related to e-safety.
- Work with the school for the implementation of policies that pertain to students and parents.
- Encourage the implementation of e-safety norms prescribed by the school for the home environment.
- Work with the school in the promotion of digital citizenship and responsible behavior.
- Alert the school in case of any issues that come to the attention of the parent rep.
- Be a spokesperson for the school when it comes to e-safety.

Roles and Responsibilities of Student Representatives:

- Take the lead in the planning of events and activities to create student awareness about e-safety.
- Actively participate and contribute to the digital citizenship program.
- Come up with ideas for improving student responsibility when it comes to the use of digital technology and discuss the same with the group to convert it into a concrete plan of action.
- Contribute to e-safety policies via inputs shared through the Students Online safety group.
- Keep track of all records and minutes of their meeting with the Students Online safety group and report it to the online safety leader.
- Report any trends or incidents that would have come to their purview to the online safety leader.
- Assist the teachers in the conduct of opinion polls, surveys, and campaigns.

Online Safety Education for Students

- Ensures that online safety education and practices are embedded across the curriculum and promoted, encouraged, and supported by all teaching staff.
- Ensure a comprehensive stand-alone curriculum is developed for online safety education which addresses the wider aspects of online safety including digital citizenship.
- Ensure that students are actively involved in promoting, designing, and delivering online safety programs.
- Ensure that online safety policies and programs are informed by students' skills, knowledge, and understanding of new technologies.
- Ensure student involvement through Digital Leaders and Online Peer Support programs.
- Oversee student surveys/feedback opportunities on online safety issues and ensure the data are collected, analyzed, and used effectively to inform online safety education programs.
- Engage students in participating in parent information sessions and promotional videos.

Staff Training

- Facilitate training and advice for all staff including non-academic staff
- Implement regular online safety training for all members of staff (including as part of the induction program) that is integrated with all other school policies and processes including safeguarding and child protection
- Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum; promoting the responsible use of technology and empowering students to keep themselves and others safe online.
- Support staff to actively engage with local and national events to promote positive online behavior, e.g.: E-Safety programs, ICT month, and anti-bullying week.
- Revise and review staff training programs to ensure they are delivering up-to-date information that reflects current best practices and are appropriate for the school community
- Ensure that evaluations of staff training are used to inform future developments of these programs
- Ensure that their knowledge and skills are refreshed at regular intervals to enable them to keep up-to-date with current research, legislation, and trends.

- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Facilitate further and more detailed training for themselves and other key staff (e.g. Child Protection Officer)

Parental Engagement and Online Safety Awareness for the Wider Community

- Promote a commitment to e-safeguarding throughout the school community
- Promote active participation by parents in the online safety of their children
- Ensure that awareness programs and information sessions are provided for parents
- Ensure all necessary documents are shared and available for current and prospective parents
- Ensure that online safety is promoted to parents and the wider community through a variety of channels and approaches such as videos, live online information sessions, documents, and posters shared on school social media, website, and official communication platforms
- Liaise with the Government Authorities and relevant agencies on matters related to e-safety
- Ensure all staff take active responsibility for online safety
- Ensure there are clear and accessible means for parents to report any online safety issues or concerns
- Ensure that parents are aware of, have read understood and acknowledged the Acceptable Use Policy for Students

Monitoring of Online Safety Incidents

- Oversee the implementation of effective reporting procedures so that all members of the school community are aware of how to report incidents and can do so quickly and easily.
- Ensure that online safety incidents are logged in a secure location and the logs are kept up to date
- Ensure that interventions are appropriate and effective in the case of any identified safeguarding issues that may arise
- Ensure privacy and confidentiality of issues logged including highly sensitive information and issues of child protection

- Facilitate regular review of all monitoring records and ensure the Principal and SLT receive regular reports
- Implement a clear process of reporting incidents to parents
- Ensure that any serious incidents concerning online safety are informed to the Principal and are reported to relevant external authorities where necessary

PHSE (Personal, Social, Health, and Economic)

The promotion of learners' personal development, (including their social development) is a fundamental aspect of education and underpins all other learning. Through our school curriculum, environment, and ethos, we promote learners' emotional well-being and self-esteem and help them to form and maintain significant and rewarding relationships based on respect for themselves and others, at home, school, work, and in the wider community.

Aims

- To promote the spiritual, moral, cultural, and social development of all learners at the school;
- To promote the mental and physical development of all learners;
- To prepare learners at the school for the opportunities, responsibilities, and experiences of life after school; Objectives to enable all learners to:
- Know and understand what constitutes a healthy lifestyle
- Be aware of safety issues
- Understand how to identify and form healthy, positive relationships with others
- Have respect for others regardless of race, gender, differences or disabilities
- Be independent and responsible members of a democratic society
- Play an active part in decision-making
- Develop self-confidence and self-esteem
- Make informed choices regarding personal and social issues
- Develop good relationships with other members of the school and the wider community

- Develop positive learning behaviors

Links with other policies and practices

The online safety policy links with many other policies, practices, and actions:

ACCEPTABLE USE POLICY

Al Resalah International School of Science (RISS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

The Acceptable use policy aims to ensure that all Students and Staff are aware of the risks and hazards of internet usage and use it sensibly and safely for information sharing and improved learning. All students and staff should know about the Acceptable use of technology. All students and staff should be free of any fear of cyberbullying by anyone known or unknown, should be able to recognize cyberbullying, and be fully equipped to be able to deal with it effectively as well as are fully competent in surfing the internet safely.

The legal underpinning of the Policy

- School is dedicated to complying with the UAE Federal law no.2/2006 dated 3/1/2006: The 'Prevention of Information Technology Crimes' provides clear guidelines regarding what is permissible and what is punishable in the usage of cyberspace. The school also assumes the responsibility of raising awareness against cybercrimes, especially against children, and training students, parents, and staff to be smart digital citizens.
- The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring, and publishing photos and comments on social media (Instagram and WhatsApp) that undoubtedly show defamation of individuals or staff members or School Leadership of character, dignity and integrity are breaking the law.
- This policy describes the acceptable use of digital technology. It is designed to minimize the risk to students, protect employees and the school from litigation as well as maintain levels of professional standings. The policy is designed to ensure the safe and responsible use of electronic

devices by all users, both on the school premises and elsewhere in which the school is represented.

- To use the school's digital resources, they must follow the guidelines outlined in this policy. The rules written in this agreement are not all inclusive. RISS reserves the right to change this agreement as and when it deems it necessary to do so.
- It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school.
- By using any digital resources, whether owned personally or by the school, users acknowledge their understanding of the Electronic Devices / Digital Resources / BYOD Agreement as a condition of using such devices and the Internet.
- The school provides some electronic devices and services to promote educational excellence.
- The school has a responsibility to maintain the integrity, operation, and availability of its electronic systems for access and use. Whilst on site, access to the school network and the Internet should be considered a privilege, not a right, and can be suspended immediately, without notice.
- Access on site is available only for educational and administrative purposes.
- Digital resources are to be used per this Policy and all users will be required to comply with their regulations.
- The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this Policy.
- This policy applies to all digital resources, not only the computers, devices, and equipment provided in the school's IT labs but also the personal devices students bring to school per the school's Bring Your Own Device initiative.
- The purpose of the 'Electronic Devices / Digital Resources / BYOD Acceptable Use' Agreement is to ensure that all students use technology in school, at home, and elsewhere, effectively, safely, and responsibly, to facilitate learning on a 24/7 basis, and to help ensure that they develop the attributes of competent digital citizens.

Strategies for Managing UNACCEPTABLE USE

Violations of this policy may have disciplinary repercussions, including:

- The School reserves the right to terminate any user's access to the School's Internet Systems - including access to School e-mail - at any time.
- If a student violates this policy, appropriate disciplinary action will be taken consistent with the Discipline policy of the School and UAE by law for the Student Code of Conduct.
- If a student's access to the Department's Internet System is revoked, the student may not be penalized academically, and the Department will ensure that the student continues to have a meaningful opportunity to participate in the educational program.
- Staff violations of this policy will be handled by suitable disciplinary measures.
- All users must promptly disclose to their teacher, parent, or line manager any information they receive that is improper or makes them feel uneasy.
- Removal of the Internet and IT Systems privileges for a period of time Temporary/Permanent removal of the students from school Temporary/Permanent removal of staff from school Suspension/Termination from school after investigation process Referral to the relevant authorities.

Reporting

All members of the school community are required to report any Unacceptable Use of technology within the school or on the school Internet or IT Systems. Any student or staff should report any Unacceptable Use or Cyber Bullying to the supervisor or to the social worker.

ACCEPTABLE USE POLICY AGREEMENT

All users must follow the Acceptable Use Agreement. **Refer to RISS ACCEPTABLE USE POLICY for more details**

Mobile Technology Policy/BYOD Policy

- Mobile Technology is an integral part of modern life and as such should be a part of School life. Bring Your Own Device (BYOD) offers a valuable resource and has numerous educational opportunities.

- As with all technology it can present risks if used inappropriately. Embracing the use of mobile technology can cause some concern, but if used within the safety of an agreed usage policy and some simple boundaries these risks can be reduced and benefits achieved.
- The word device is used to describe any mobile phone, tablet, laptop, or device capable of communicating with either the Internet or recording information.
- Use of personal BYOD devices is at the discretion of the School and should not be seen as an automatic right.
- The aim of the Mobile Phone Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines.
- This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools.
- This policy outlines the acceptable use of mobile technology at RISS in the context of safeguarding. We recognize the vulnerability of our students and the potential for exploitation and abuse through the Inappropriate use of mobile phones.
- We take steps to ensure that our safeguarding procedures are all-encompassing and robust.
- It is recognized that it is the enhanced functions of many mobile phones that cause the most concern, offering distractions and disruption to the working day, and which are most susceptible to misuse – including the taking and distribution of indecent images, exploitation, and bullying. However, as it is difficult to detect specific usage, this policy refers to ALL mobile communication devices.

At RISS we recognize that mobile phones play an important part in our lives and when used as they are intended, can bring substantial benefits. We also acknowledge that there is a risk that they can be used for the taking, storing, and using of images inappropriately in a way that
denies students' right to dignity, privacy, and respect.

Refer to RISS Mobile Technology Policy/BYOD Policy for more details DATA

PROTECTION POLICY

- RISS School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school.
- This information is gathered in order to enable the school to provide education and other associated functions.
- In addition, there may be a legal requirement to collect and use the information to ensure that the school complies with its statutory obligations.
- All staff involved with the collection, processing, and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

PURPOSE

This policy explains the general principles that will be used by RISS in processing data and how you can complain if you feel that we have used your data incorrectly. The appendices explain, for specific types of data, how and why personal data will be used and how long it will usually be retained.

DATA PROTECTION PRINCIPLES

We will comply with data protection laws and principles, which means that your data will be: Used lawfully, fairly, and in a transparent way. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes. Relevant to the purposes we have told you about and limited only to those purposes. Accurate and kept up to date. Kept only as long as necessary for the purposes we have told you about. Kept securely.

GENERAL STATEMENT

The school is committed to maintaining these principles and will therefore:

- Inform individuals why the information is being collected and when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and accuracy of the information it holds Ensure the information is not retained for longer than necessary
- Ensure that when obsolete information is destroyed it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, and unauthorized disclosure, irrespective of the format in which it is recorded

- Share information with others only when it is legally appropriate to do so Set out procedures to ensure compliance with subject access requests
- Ensure our staff are aware of and understand our policies and procedures

EMAIL PROTOCOL AND EMAIL POLICY

- This policy applies to all users of Al Resalah International School of Science email system, whether through a PC, laptop, tablet and laptops, or any other hardware device.
- It includes Administrative Staff as well as staff and applies equally whether you are working from school, at home, or from this guidance m any other location. These groups of people will thereafter in this document be collectively referred to as users.
- The school must be able to communicate quickly and efficiently with employees and has established email as a means of communication.
- All employees are provided a riss.ae email account to which the school will send official email communications.
- Users must follow the Email communication Protocols If there is evidence to suggest that users have not followed this policy it may result in an investigation leading to loss of email facilities or additional disciplinary actions within the school and according to the U.A.E laws.

SECURITY POLICY

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Al RESALAH INTERNATIONAL SCHOOL resources. All users, including students, staff, and parents with access to RISS systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all students and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any RISS

facility, and has access to the RISS network. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, and network logins.

General

- All systems-level passwords (e.g., network administrator, application administration accounts,
- Teachers account, students account, etc.) must be changed at least every 30 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days and cannot be reused the past 10 passwords.
- User accounts with access to the school website must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

FILTERING AND MONITORING POLICY

Purpose

This policy sets out the principles to maintain and support research, teaching, and other business activities whilst protecting users, networks, and computers from unwanted network traffic and illegal or other content in breach of the regulations of UAE Data and privacy protection.

Scope

This policy covers all Staff, students, Partners, Parents, and visitors using the RISS network. This policy applies to all communications between the School networks and the Internet, including web browsing, Applications, instant messaging, file transfer, file sharing, and other standard and proprietary protocols.

Policy

Through the use of firewall and web filtering technologies, the Al Resalah International School prevents access to certain categories of websites via its networks, as set out below. In compliance with the Data and privacy protection in the UAE and Internet Access Management (IAM) policy, Al Resalah International School has adopted and enforced this Internet content filtering policy that ensures the use

of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all devices under Crown Private School network with Internet access.

The current Content Classification System provided through the School's firewall allows for automatic site blocking based on a range of categories e.g. 'Adult', 'Hacking', and 'Extremism'. The list provides an objective categorization of sites and is actively maintained by the firewall vendor.

Social Media Policy

- All members of the RISS community are expected to uphold the values of the school in all Social Media interactions.
- Staff, students, and parents will not act in such a way that the image of RISS is brought into disrepute nor in a way that harms members of the school community.
- Therefore, it is expected that RISS staff, students, and parents use Social Media in a respectful and responsible manner.
- Social Media should not be used to insult, present offensive or inappropriate content, or misrepresent RISS or any member of the school community.
- Social Media includes blogs, wikis, podcasts, digital images and video, instant messaging and mobile devices.
- Due to the wealth of new social media tools available to students, student products and documents have the potential to reach audiences far beyond the classroom. This translates into a greater level of responsibility and accountability for everyone.

Induction Policy

We should ensure that an induction is provided personally, by the line manager or mentor, or another person with delegated responsibility and is tailored to each individual. All new staff will be given appropriate induction advice, and training over a period of time and as necessary.
Areas which should be considered are set out below. These are not intended to be exhaustive and careful consideration should be given in relation to each post and the experience of the post holder.

- Safeguarding children and child protection information
- Health and safety procedures
- Fire and emergency procedures

- First aid
- Code of Conduct
- Staff Handbook
- School Website
- Policy documents
- Acceptable use agreements
- Assessment advice, recording, reporting, resources and procedures
- Information on whole school and year group data, including SEN
- School administrative systems and procedures (for admin staff)
- Details of help and support available
- Designated mentor or supervisor

New employees and students:

All users remain informed of our expectations and appropriate usage of resources through an induction program.

The E-safety team will:

- ensure all new students and staff receive access to age-appropriate ICT resources and tools during the enrollment and hiring process, as well as ongoing training in their safe, responsible, and effective use; and
- Provide orientation annually for students and staff on ICT resources and the school AUP.