www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

RAHA INTERNATIONAL SCHOOL
KHALIFA CITY CAMPUS

POLICIES

Policy title	Taaleem E-Safety
Policy number	KCC_POL_ES_01
Policy Version	1
Effective date	August 2023
Scheduled review date	August 2024

Prepared by
Taaleem

Approving Committee	Name	Signature
Principal	Nicola Neethling	

www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

Table of Contents

Policy Statement

KCC provides online services to students for learning-related support, pastoral care and counselling activities. Schools provide access to quality virtual learning technologies within a duty of care framework, thus ensuring all such activities occur within an environment of student safety and well-being.

Our school make every reasonable effort to educate and protect students from exposure to inappropriate online material and activities. This policy acknowledges our commitment to keeping children safe online and complements the school's overall Safeguarding policies and procedures.

www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

The policy covers:

1. School-Provided Online Services

Including, but is not limited to, email, calendar, instant messaging, web conferencing, web meetings, on-line discussion groups, online file sharing and storage, learning management systems, e-learning platforms, blogs, podcasting, web browsing, gaming and monitoring the content browsed on BYOD that may be accessed using the computer networks and services of the school.

2. Inappropriate Content

Content that is considered unsuitable or harmful to students such as material that is racist, sexist, inflammatory, threatening, pornographic, hateful, obscene, or abusive in nature, promotes or encourages illegal activities or violence.

3. Learning-related Activities

School activities that are part of the planned class and/or whole school education of a student.

4. Third Party Services Providers of Online Applications

Third Party Service Providers are those who render an online service or product to the school.

Policy Administration

KCC will:

- Communicate the requirements of the policy and procedures to all staff involved with the provision of online services.
- Ensure all staff and volunteers read and sign the 'Staff Acceptable Use of Technology & Social Media Agreement' before using any school ICT resource. These agreements form part of the employee's file.
- Ensure parents are aware of the policy, understand it and are involved in keeping their children safe online.
- Only grant students access to online services after receiving an 'Acceptable Use Agreement of Technology & Social Media Agreement' signed by their parents.
- Ensure that the software chosen Is secure and has the relevant privacy and security

settings in place.
- Issue and maintain student passwords in accordance with the Taaleem IT security policy.
- Confirm students have received education about the risks and their responsibilities when accessing the school's online activities.
- Provide appropriate supervision for students using online services for learning related or support activities on school sites.
- Take appropriate action in accordance with the School's Behaviour Policy and Child Protection Policy where there is a breach of acceptable use.
- Apply the requirements of this policy and procedures when using Third Party Service Providers.

Responsibility for Implementation and Compliance of the Policy

The school Principal is responsible for implementing the policy and monitoring its compliance.

Complaints of internet misuse by students will be dealt with by the school's Senior Leadership Team. Any complaint about staff misuse must be referred to the school Principal. Any complaint about school Principal misuse must be referred to the Director of Education.

School Procedures

1. Consent and acceptable procedures

Ensure all students have signed parental permission to access an Online Services account, and a signed Acceptable Use Agreement in order to access school provided services.

2. Student Personal Security

- Ensure all staff involved with learning related online services have taken adequate steps to fully inform students regarding personal security protocols such as keeping passwords secure in an online environment.
- Students only use approved e-mail accounts in school which are deactivated upon leaving.
- Display e-safety rule posters in the classrooms.
- Students to be fully informed of the minimum age, and other protocols pertinent to accessing social networking sites.

www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

3. Responsible Online Practice

- Ensure all staff involved in learning or support related online services are kept up to date with the relative risks and educational benefits of online activity.
- Ensure the school's filters block sites which are deemed to contain inappropriate material or content.
- Ensure the school's ICT systems capacity and security are reviewed regularly.
- Ensure virus protection is installed and updated regularly.

4. Personal Information, Privacy and Confidentiality

Ensure staff have fully informed students about the risks associated with any online activities, and how to adopt protective online behaviours to protect themselves.

Such behaviours include, but are not limited to:

- Understanding their rights as a child for safety, respect and privacy.
- Identifying behaviours online from adults or students which are inappropriate or unsafe.
- Seeking help from people within their trusted adult network.
- Knowing where to find support when they are being cyberbullied or receiving unwanted contact.
- Using appropriate practices for the physical and logical storage, and security of digital information, such as not storing private information on public websites.
- Applying appropriate protocols when using ICT to safely create, communicate or share information such as posting to social media.
- Never publishing or disclosing the email address of a staff member or student without that person's explicit permission.
- Exercising vigilance and caution when revealing personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.

5. Publishing Student Images and Information

- Publish work or images of students is permissible only after parent permission is received
- Ensure any material planned for publication on the internet or intranets has appropriate copyright and privacy clearance

www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

6. Third Party Services Providers of Online Applications

Emerging technologies will be examined for educational benefit by the school, and a risk assessment undertaken before adoption by the school

Third Party Service applications, such as Google Apps for Education, Seesaw, Studyladder, Edmodo, Skoolbag, Reading Eggs, Mathletics, ClassDojo and Remind may be accessed via websites or downloaded from reputable retailers such as Apple iTunes or Google Play. Third party social media services, which may also hold personal information, could include Facebook, Instagram and Twitter.

7. Student Misuse and Breach of Acceptable Use

The school will take appropriate action in accordance with the School's Behaviour Policy and Procedures and Child Protection Policy and Procedures, where there is an alleged misuse of online services, or breach of acceptable use. It will:

- Follow procedures for fairness and due process, where there is an alleged misuse, or breach of acceptable use. The school will investigate the reported misuse, and where possible, identify the offender and institute appropriate action
- Disciplinary action will be commensurate with the nature of the policy breach (for example counselling, parental involvement, police involvement), and additionally promote, and develop the necessary self-discipline required in utilising online learning tools.
- Promptly address the online publication of defamatory material about staff or students by keeping a record of the nature and location of the offensive inappropriate material and hiding/removing/deleting it wherever possible.

8. Receiving Inappropriate Material from Students

The school will communicate to staff steps to take and advice to give if students notify them of inappropriate or unwelcome online activity by fellow students or members of the public.

Staff Guidance on Professional Conduct Online

KCC employees must adhere strictly to the instructions below:

- Only use school approved platforms and communication channels.
- Ensure the students stay within private online communities.
- Maintain professional conduct and treat each online lesson the same as a classroom lesson
- Dress appropriately and sit against a plain background which does not display any

private information.

- Distribute a class timetable / schedule for e-learning.
- Teach content that is age-appropriate, flexible, relevant and engages student interest. Give students regular feedback.
- Consider the needs of SEND students and vulnerable learners.
- Ensure live lessons take place with the whole class bearing in mind that some students may work slower than the others.
- If you need to interact with a student 1 on 1 ensure you are doing so in the presence of the parent / caregiver or a member of the school's senior leadership team.

Staff Guidance on the Use of Social Networking

Taaleem employees must adhere strictly to the instructions below:

- Never engage with students from the school in any form of social media. Additionally, it is strongly advised not to engage on social media with ex-students who are still minors.
- Refrain from using personal emails or numbers.
- Refrain from communicating outside of school hours.
- Staff who engage with social media sites, such Facebook, Twitter, Instagram etc. need to be aware that they are representatives of the school and should not engage with or post comments which affect the professional identify of the school, can be considered inappropriate or defamatory in nature, be it libelous or slanderous.
- Staff are required to follow policy instructions and demonstrate acceptable conduct when using the school's IT systems. Posting of student photographs and/or other identifiable information is not allowed without prior approval from the Principal. In case of misuse or unprofessional conduct the local authorities will be informed.
- Staff may only take photos in school, for school use, on school provided iPads or technology and not on personal devices. This also applies to all third-party service providers.
- Any images of students posted on the school website or school authorised literature (e.g. brochures), must have the required parental permission.

Parent Guidance on Professional Conduct Online

- Position the computer or webcam in a public space at home, preferably not in a bedroom. Try to keep the background neutral with good quality light and sound.
- Ensure only official school communication channels are used.
- Remind your child to not share passwords or other sensitive information.
- Establish a daily schedule and routine.

www.ris.ae
T: +971 (0)2 550 5271
Abu Dhabi, United Arab Emirates

- Take an active interest in your child's online learning.
- Be available to help your child and monitor their progress.
- Be aware of the privacy and security settings to ensure communication is secure.
- Ensure parental controls are in place for children to conduct online searches and activities.
- Maintain feedback with the teachers.
- Do not use the school platforms to discuss personal matters.
- Look after the child's mental health and well-being.

Revision Log

Date	Changes	Reviewed By