Ras Al Khaimah American Academy				
Subject: Online Safety Policy			**SOP No: RAKAA-WS001**	**Controlled Copy No:**
			Revision No: New	
Written by:	**Online Safety Leader/Principal**	**Date:**	**Policy based on:** Best practices for RAKAA's safeguarding obligations as per eSIP.	
	Sandra Zaher	Jan 2022		
Checked by:	**ICT Manager**	**Date:**	**Supersedes:** New	**Issued on:** April 11, 2022
	Ms. Asma and Mr. Naveed	April 2022		
Approved by:	**Online Safety Leader Assistant**	**Date:**	**Distributed to:** Whole School OSG, SLT, Parent, Teachers, Students	**Pages:** 24
	Mrs. Farhat and Ms. Katie	April 2022		
Authorized by:	**Principal**	**Date:**	**Policy effective as of:** April 11, 2022	
	Sandra Zaher	April 11, 2022	**Policy review date:** Annual – April 11, 2023	

Contents

Online Safety Policy Objectives

The RAKAA Online Safety Policy was by the RAKAA learning community and written by the RAKAA school principal based on the previous E-Safety School Policy and the updates received from the MoE for eSafe framework in UAE schools aligned with the eSchool Improvement Plan objectives for best practices that is aligned with the new updated MoE Framework for schools (academic) and the COGNIA (academic) Framework to ensure national and international best safety practices for K-12 learning environments.

1) This policy reflects the aspects and follows the policies of the Ministry of Education, and the UAE Cybercrimes polices (1) and Article (11) of the Federal Decree-Law No. 34 of 2021 on combatting rumours and cybercrimes, of the UAE Government (2),
Emiri Decree No.02 of 2018 (3), and the Internet Access Management Regulatory Policy (4).

RAKAA's purpose for use in our school is to:

- Strive to ensure that all members of the RAKAA learning community are protected, educated, and understand the regulations that are in place when accessing the internet at RAKAA (on campus) or off campus keeping our RAKAA learning community and the wider RAK community when using technology of any type and instilling a high sense of security and knowledge that at RAKAA online safety is priority and ensuring all a high level of online security.
- Educate and increase understanding of what online safety means and why it is important for positive safe learning environments throughout the school.
- Inclusion of all stakeholders, empowering students/parents/teachers/staff in a shared understanding of digital security and online safety that follows the RAKAA and UAE regulations while online accessing sites on the Internet.
- Empower students to create new ways to identify their needs (what they want to learn new about eSafety, Digital Citizenship, UAE and Internal online regulations, to work with the RAKAA Online Safety Group and guide student education of best safety practices aligned with Acceptable Use Policy as role models for others within the school community.
- Identify and layout procedures for the RAKAA community to follow in the event that there is an online safety issue, threat, or concern.

The risks categories that this policy will help the RAKAA community to recognize and ensure best practices are followed to protect when accessing the internet. RAKAA will focus on:

1) **Education/Communication.** This category is combined as both are needed for all members of the RAKAA learning community to ensure the understanding of the 'Whole School Ownership" when using technology that follows the Online Safety Policy, the Online Safety Education Policy, the Acceptable Use (unacceptable use) Policy to increase awareness and potential possibility to exposure to harm via use of the internet.

2) **Risks Management**: This category ensures the understanding of the
Online Safety Policy and the Acceptable Use /Unacceptable Use Policy and the consequences or sanctions of accessing unacceptable or illegal sites or actions online that could be potentially harmful to the RAKAA learning community.

Scope of the Online Safety Policy

At Ras al Khaimah American Academy (RAKAA), our priority is safety to all within the RAKAA learning community and extends to the community beyond. Priority number one is our students. Our school's policies and interactions with technology through teaching and learning are embedded with knowledge from students, parents, teachers, staff, and admin of UAE internet use regulations and RAKAA policies, guidelines, and consequences/sanctions if these polices, and regulations are breeched. The RAKAA Online Safety Policy follows the UAE Future Skills for Youth which states:

"Problem-solving, critical thinking and interpersonal skills like empathy and collaboration are the skills needed for future workforce. Artificial intelligence, robotics, automation and advanced manufacturing, virtual reality, augmented reality, big data, alternative energy and waste management will shape the skills required in future. Read about the special programmes for developing future skills." (9)

The Online Safety Policy is age appropriate cascaded to ensure that all cycles of learning within RAKAA can grow and develop an understanding of online safety- what is acceptable, what is unacceptable, and why there are consequences/sanction for the unacceptable use of technology.

As our school grows and develops further in this rapidly changing world of technology, so will our need to revise and revisit UAE national amendments to Internet Use Laws and amend our policies to match required regulatory changes made by the UAE. Strategic plans for the increase in technology in the world beyond RAKAA further drives the need for teaching solid safe online teaching and learning practices. The Abu Dhabi Future Skills Report 2030 Report drives the RAKAA educational strategic plans as the ADFSP 2030 states in the future:

"Freelancers will not be able to rely on traditional HR departments, onboarding processes, and many of the other affordances of institutional work" (IFTF/ Dell). Therefore, adaptation and learning skills will be increasingly important as workers will need to take charge of their learning journey. This continuous learning process will be mostly digital, allowing them to seamlessly access a myriad of courses and videos on nearly any topic." (10)

The RAKKA Online Safety Policy applies to the entire RAKAA Learning Community including anyone who access and uses the school's learning/management or visitor who accesses to our RAKAA online systems. This applies to on-campus and off-campus access/use RAKAA online technology systems.

Online Safety Policy

The RAKAA Online Safety Policy recognizes and follows UAE national and internal regulations as well as being linked to other RAKAA policies. (Links accessible in References)

- Child Safety and Protection Policies
- Federal Law 216- Wadeema's Law UAE
- RAKAA Behaviour Policy
- Student Behaviour Management Distance Learning 2020 (MoE)
- Student Code of Conduct (MoE)

- Abu Dhabi Future Skills Report 2030 Report
- UAE Future Skills for Youth Strategies
- Cyber-Bullying and Anti-Bullying
- Acceptable Use Policy and Agreement
- Unacceptable Use Policy and Agreement
- Personal information and Confidentiality Policy
- Password, Filtering, and Monitoring Policy
- Social Media and Digital Policy (UAE)
- Digital Participation Policy (UAE)
- Human resources regulations (UAE)
- Federal cybercrimes law (UAE)

Policy Development and Review

As per the RAKAA Board of Trustees guidelines regarding policy review the RAKAA Online Safety Policy will be reviewed as needed as per changes in UAE or International eSafety laws and will be updated monthly to reflect any RAKAA, RAK, UAE or International Child Protection or Online Safety or technical updates required to ensure child and community safety and protection when interacting with technology at RAKAA. Further an importance to provide futuristic teaching and learning requirements the school policy is considering the new and emerging technologies while updating and developing policies impacted by the rapid changing age of technology such as Telegram, Twitter, TEAMS, MoE Smart Learning Portal,

Continuous review and development of the Online Safety Policy

Policy review process of the Online Safety Policy to ensure that safe internet and online safety procedures are fully in-place and implemented across RAKAA following the eSIP, SIP, and OSP.

- Priority: Education of policy cascaded to all understand, know and follow the Online Safety Policy and Procedure
- RAKAA IT, monitor the access and use of the school system following filtering, monitoring, and reporting protocols to ensure that the OSP is enacted.
- The school principal/vice principal and OSL/OSLA/Child Protection Officers responsibilities to ensuring a safe learning environment are strengthen as supported by policy, procedure, and review ensuring a high level of safety and online safety precautions.
- Online Safety Officer to submit periodic reports to Board of Trustees about online incidents and its consequences.
- IT submits a weekly report to the school principal reflecting policy breeches, filtering, and monitoring as mandated in the eSIP.
- ESafe Schools development plans have appropriate precautions for online safety.
- Involvement of school community as part of the review of policy

- Development of an awareness within the school among all within the RAKAA learning community, that whole school community accountability and awareness of acceptable use in and out of school.
- Include the online safety policies and updates in the eSafe and Academic School Development Plans.

Separation of Roles and Responsibilities

This part of the policy defines the roles and responsibilities for online safety of RAKAA as a whole school collaboratively through individual and groups within the RAKAA learning community.

RAKAA Board of Trustees:

The RAKAA BoT are responsible for approving the RAKAA Online Safety Policy and auditing and reviewing its effectiveness. It will be carried out by the BoT receiving regular updates and information about online safety and RAKAA and monitoring reports provided by the Online Safety Lead in conjunction with the Online Safety Group (the BoT member who has been appointed as Online Safety Director.)

The Board of Trustee Member in their capacity as Online Safety Director is responsible for:

- Conducting regular meetings with the Online Safety Leader (OSL) or Online Safety Lead Assistants (OSLAs)
- Periodically attending Online Safety Group meetings
- Regularly monitoring the RAKAA online safety incident logs
- Regularly monitoring filtering and change of control logs.

Principal of RAKAA

The Principal of RAKAA has a duty of care towards all members of the RAKAA community to ensure their physical and online safety.

- The principal has the ultimate responsibility of following the procedures to be followed in case of a serious online safety allegation being made against any member of staff. (Refer to the flow chart on dealing with online safety incidents).
- Meets with whole school concerning safety of both online and on-campus learning environments to ensure that the policies of the school and learning community are understood and in place. Examples but not limited to: Child Abuse Policies, Behaviour Policies, Acceptable Use Policy, Unacceptable Use Policy,
- At RAKAA, the Principal has also assumed the role of Online Safety Leader. (Refer to the Roles and Responsibilities of the OSL

The Principal at RAKKA is responsible for ensuring that the Online Safety Lead Assistants (OSLA's) and members of the Online Safety Group, receive appropriate training to enable them to carry out their online safety roles and to train other colleagues, as needed.

- 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 online safety monitoring role so that they have the support needed when carrying out their important monitoring roles and provides a safety net if needed. The Senior Leadership Team (SLT) and BoT will receive regular monitoring reports from the principal in the capacity of Online Safety Lead.

Online Safety Lead (OSL) and Online Safety Lead Assistant (OSLA)

At RAKAA, whilst the Online Safety Lead has the overall responsibility for Online Safety in the school, it is important to have an Online Safety Lead Assistant who is able to be onsite and take on the roles and responsibilities of the OSL should she become unavailable.

The OSL or OSLA will:

- Lead the Online Safety Group (OSG)
- Take responsibility for online safety issues at RAKAA on a day-to-day basis and take the lead in creating and reviewing the RAKAA online safety policies and documents.
- Ensure that all members of the RAKAA community are aware of the reporting procedures that must be followed in the event of an online safety event occurring.
- provide regular CPD sessions to communicate and educate the online safety policy to all in the RAKAA learning community (students, parents, teachers, staff, administration, volunteers, visitors, and the external community) stakeholders.
- Liaises with the MoE and other relevant bodies with regards to monitoring and inspection of RAKAA online safety.
- Liaise with the RAKAA ICT Department to receive reports of breaches of acceptable use, review reports related to online safety, and create a log of incidents to be used to inform future online safety developments within the school.
- Regularly meet with the BoT member for Online Safety, Dr. Suleman in order to review incident logs, discuss any current issues and filtering and changing control logs.
- Attend BoT meetings to update them on current issues and needs to maintain consistency in the standard of online safety at RAKAA.
- Attend meetings with the SLT and report any issues and collect feedback from different departments with regard to Online Safety.
- Receive reports from the ICT department when a Student/Parent or Staff Member has reported online safety issues and determine the relevant steps to take when investigating the matter.

ICT Managers:

The ICT Managers at RAKAA are responsible for:

- Ensuring that the RAKAA technical infrastructure is securely maintained and is not open to any misuse or malicious attacks.
- Making sure that RAKAA is able to meet all required online safety technical requirements and any guidance that is issued by the Ministry of Education (MoE).
- Ensuring that users may only access the RAKAA network and its devices via a strictly enforced password protection policy, as well as ensuring that passwords are changed on a regular basis.
- Strictly enforcing the RAKAA Filtering Policy and updating it on a regular basis. The department will ensure that the implementation of this policy is not the sole responsibility of any one person within the department.
- Keeping up to date with developments in online safety technical information so that they are able to effectively carry out their online safety role and provide advice and guidance to other RAKAA stakeholders when it is relevant.
- Ensuring regular monitoring of the RAKAA networks, Learning Platforms, VLE and email so that any misuse or attempt to misuse can be reported to the OSL for investigation and sanctions to be applied where necessary.
- Ensuring that monitoring software or systems are implemented and maintained regularly as best practice.

RAKAA Teaching and Support Staff

At RAKAA the educational and support staff must:

- Read, understand, and sign the RAKAA Staff Acceptable Use Policy and follow the stipulations set out within it in their day-to-day practice.
- Maintain an up-to-date awareness of online safety matters and of all current RAKAA policies relating to Online Safety and practices via CPD sessions and through reading emails with advice from the ICT department.
- Report any suspected misuse of Online Safety issues to the ICT department via this link https://forms.office.com/r/bhW2thQhAb so it can then be processed and forwarded to the OSL for investigation and sanctions applied where necessary.
- Ensuring that all digital communication with students and parents from educators is conducted using the sanctioned school platform of Microsoft Teams wherein all correspondence can be monitored and tracked.
- Creating opportunities for online safety issues to be regularly discussed within their classrooms via ICT lessons, Digital Citizenship lessons, and other areas of the curriculum so that it becomes embedded within the fabric of the curriculum and school.
- Ensuring that all students in their Homerooms understand and follow the RAKAA Online Safety Policy and the Students Acceptable Use policies.
- Providing students with a thorough understanding of research skills and the importance of avoiding plagiarism within assignments and maintaining copyright regulations.

- Making sure that they monitor the use of all digital technologies within their classrooms or lessons and implementing all policies linked to the Online Safety Policy with regard to these devices.

Online Safety Group (OSG)

- The RAKAA Online Safety Group is a consultative group formed by members of the teaching staff, the ICT department, students from the E-Safe School Initiative, members of the BoT, and the OSL and OSLA's, the Child Protection Officer, and members of the RAKAA PTA. It has been formed to include a wide representation of the RAKAA community so that it can take responsibility for any issues associated with online safety and the monitoring and improvement of the Online Safety Policy. The RAKAA OSG will be reporting regularly to the RAKAA BoT.

RAKAA Online Safety Group is responsible for assisting the OSL and OSLAs

- the production, review, and monitoring of the RAKAA Online Safety Policy and its related documents.
- the production, review, and monitoring of the RAKAA School Filtering Policy and requests for any filtering changes.
- Mapping and reviewing the online safety curricular provision to ensure that it is relevant and has a wide breadth and natural progression as students grow from KG-12.
- Monitoring the RAKAA network internet and incident logs.
- Consulting with relevant stakeholders which includes our students and their parents about the online safety provision at RAKAA.
- Monitoring improvement actions identified in the RAKAA School Improvement Plan.

Students:

- All students at RAKAA are responsible for using the school's network and devices in accordance with their age-appropriate Student Acceptable Use Policy.
- All students must understand the importance of reporting abuse, misuse or accessing inappropriate materials and know that they can scan the reporting posters in each Homeroom or common areas around the school to report concerns.
- All students will be expected to know and adhere to the policies on the use of mobile devices and digital cameras. They must also be aware of the school's policy with regard to taking photos of other members of the RAKA community and the school's cyberbullying policy.
- All students should be aware of the importance of following best practice with regard to online safety when using digital technologies and understand that the

RAKAA Student Acceptable Use Policy covers their actions online both on campus and when they are out of school if it is related to their membership of RAKAA.

RAKAA Parents / Carers

At RAKAA, we understand that our parents and carers play a large and crucial role in helping to ensure that their children understand the importance of using the internet and mobile devices in an appropriate way. RAKAA will provide opportunities for parents to develop their understanding of online safety issues via parent's evenings, newsletters, providing information on our website and conducting online training via Microsoft Teams and awareness videos and leaflets produced by the RAKAA E-Safe School Initiative.

Parents at RAKAA will be encouraged to support the school in promoting best practices for online safety and the importance of following the school guidelines for the appropriate use of the Online Safety Policy, Acceptable Use Policy, Parent Engagement Policy:

- Undertaking to not interfere or interrupt live online lessons if their children are studying from home
- digital and video images taken at school events
- protecting all children's images as per UAE and RAKAA regulations/laws
- their children's personal device in school
- their use of mobile devices when on school premises

Policy Statements

Education at RAKAA

At RAKAA students' safety and learning are our priority. The use of 21st century learning tools very important as an integral part of teaching and learning on campus and online is important to sustain learning concepts and create a balance using technology. To this end, RAKAA has embedded eSafety and digital learning throughout the curriculum KG-G12.

It is our responsibility as a school to ensure that our students our children and young people are educated throughout all subjects and levels within the school curriculum with skills to enable them to know and recognize best-safe practices when using technology in school and in real life outside the school campus.

Further, it is RAKAA's duty to equip our children and young people with the skills and abilities to know safe use practices and to make proactive choices to avoid taking risks online or physically through attaining knowledge of unacceptable use and the dangers that are possible if regulations regarding online safety within their daily learning through eSafe Digital Curriculum.

At RAKAA, as a whole school, our approach is as one to reinforce online safety across interdisciplinary lines. Our eSafety curriculum uses broad strokes to teach important eSafe practices

and awareness of unsafe practices when using digital technology (both online and onsite/on-campus). Learning opportunities are provided such as:

- Delivering digital awareness lessons as part of the planned online safety curriculum
- Assembles, TEAMS class wallpaper, message in poster or digital format used to help reinforce the planned eSafety digital program.
- Key curriculum safety points will be reinforcing as part of the planned curriculum that include student understanding and reflected through the students work or comments.
- Key points and a request to assist in their child's understanding of the Online safety Policy, Best Practice and the Unacceptable Use policies are in place and addressed regularly through the PTA meetings, Parent teach Conferences, Incident meetings, parental digital safety training, and personal interaction with their own child discussing eSafe practices.
- Teachers are role models for eSafety standards and will follow the Online Safety Policy/Acceptable Use Policy ensuring best safety practices are in place by vetting websites or links prior to planning for student use. To ensure a safe in class and at home access to any link or digital reference required to complete lessons and learn how to navigate safe sites (acceptable use) and sites that have possible unacceptable content or unsafe content for themselves or their devices.
- All sites that students visit (that is part of planning for teaching and learning) have been vetted, reviewed, and approved. Teachers are vigilant and educate students about inappropriate and unacceptable use of prohibited websites.
- Teachers monitor students' online access while in their learning environment and IT monitor any attempted breeches to access blocked and prohibited sites (online and on-campus) when using the school's educational system (TEAMS).
- Plagiarism and how to paraphrase is an important part of the RAKAA education of best eSafe practices that is taught throughout the differential age of learning stages within the digital safety curriculum.
- Students are taught to critically think about making the right choice when interacting with digital content online. The school has firewalls and other strong eSafe learning environment barriers in place to ensure a safe learning space for our students.
- All students, parents, teachers, and staff are required to read, understand, and actively refer to the Acceptable Use Policy when on campus or online (even at home).

Education – Parents / carers

RAKAA has the duty and responsibility to assist parents in their understanding and knowledge of how digital content is used in school. Parents and carers need to understand the risks that are involved without parental oversight when their child is accessing online content when off campus

and they need to understand the safeguards that are possible to keep their children as safe online as possible. Parents are the key to our students learning and development. It is part of our community responsibility to offer sessions and training of our programs and the threats their children might find online safety risks and issues. Together parents and school provide guidance and role modelling in the safe education of their children. IT and the OSL/OSLA/OSGroup provide parents and students with a shared understanding and in the monitoring / regulation of the children's on-line behaviours. It is the school's responsibility to raise parent awareness to the dangers online and the tools to assist them in responding to child's curious questions or in the event of misuse of their online or on-campus digital technology use.

RAKAA provides parents understanding acceptable use and the online safety policies through:

- Scheduled recorded sessions of safe internet use.
- IT training sessions for TEAMS and mobile device use.
- Parent meetings with the OSL/Principal
- eSafety ideas at assemblies
- TEAMS communication, emails, newsletters, web site, notifications
- Highlight- eSafe events such as Safer Internet Day, ESafe School Avatar Competitions, Plagiarism FREE competitions, poster and online design competitions that promote eSafety

Education – The Wider Community

RAKAA will extend opportunities to the greater RAK community to showcase our school's online safety knowledge and experience.

- Sessions for parents in digital technologies, digital literacy and online safety
- RAKAA links to tutorials and training on eSafety Policies and other eSafety information as needed.
- Website is used to promote best practices through accessing eSafe Policies, schedules for training, and safe internet that is accessible by the greater community in RAK and UAE.

Education & Training – Staff / Volunteers

RAKAA provides all staff with online safety training during onboarding and as employees of the school to ensure that they understand roles and responsibilities, as outlined in this policy and in the acceptable use policy . Staff/volunteer training include:

- Planned sessions through HR, OLSL/Principal and the OLG using both in-person and online safety training for all staff.
- Onboarding and induction training for all new staff by the OSL/Principal/IT
- The training will be revisited each Term or as needed. But will be reinforced through eSafety Team meetings.

- An online audit through survey of training is required to drive decision making with data.

Training – RAKAA Board of Trustees

The RAKAA Board of Trustees takes part in the online safety training in several ways such as:

- Review and approval of eSafe policies
- Esafety reports made to the Board form the Principal/OSL or others
- Participation in eSafe information sessions for staff and parents.
- Discussions with the eSafety Director who is a member of the Board

Technical infrastructure / equipment, filtering, and monitoring

RAKAA is responsible to ensure that the technical infrastructure and equipment, filtering and monitoring system and network meets the UAE requirements to ensure a safe as possible teaching, learning and working online environment as reasonably possible. The school is responsible to ensure that there are approved policies and procedures in place that are known and implemented throughout the school. The following aspects of RAKAA technical infrastructure/equipment, filter ad monitoring are in place to ensure optimal safety within our learning community:

- RAKAA uses professional technical systems to support and protect uses as aligned with the eSIP and MoE ESafe Schools framework to ensure that RAKAA is in compliance with the technical requirements to effectively allow use of the RAKAA online learning by meeting the infrastructure requirements of the UAE, following the eSIP guidelines.
- RAKAA IT annual audits of the network/system in use to RAKAA to ensure highest safety possible as follows:
  - Weekly reports to OLS/Principal about the infrastructure and equipment, filtering, and monitoring system.
  - Annual audits using in at the end of each academic year to ensure that the integrity of the infrastructure and system in place. Or as needed if incident occurred and auditing is required to identify issue and make required updates to ensure complete safety.
  - Bi-Annual external audit.
- To ensure physical safety and prevent disruption or accidents the RAKAA servers, wireless router systems, and cables are protected/out of reach with physical access to unauthorized IT personnel strictly prohibited and clearly marked.

- Each different user will have different clearly defined access rights to the school technical networks/systems as defined in the Acceptable Use Policy and in job descriptions that recognize the type of user and access that is possible.
- All Users at RAKAA are provided with a username and secure password by the IT Managers. As per policy and procedure there is an automated log of uses and usernames.
- As per the Acceptable Use Policy, users are responsible to keep their username and password safe and secure as per the password policy. Based on the complexity of different age groups within the school at the lower levels in the school's parents have the responsibility to change the passwords once IT has issued to maintain the integrity of password security and safely. Teachers/staff will refer to the Acceptable Use Policy and the RAKAA Staff Handbooks for reference and guidelines that ensure password security from students or others.
- Password and filtering logs are kept for continuous review to ensure security.
- Students and staff can alert or report misuse as identified in the Acceptable Use Policy by using QR Codes designed to assist in reporting. Students can also report to, Teachers, Social Workers, Child Protection Officer, ICT Coordinator, IT, Head of Sections, and OSL/Principal/OSLA
- RAKAA IT is responsible to ensure:
  - All software license logs are up to date
  - Regularly scheduled checks of the number of licenses purchased to ensure that the number of software installations within RAKAA system are accurate and the school remains compliant so that there is no copyright breech as written in the UAE Copyright Act under Federal Law No. 7 of 2002 (8)
- RAKAA follows the Filtering Policy to ensure that the school community Internet access is filtered for all users. Illegal content as described in the Acceptable Use Policy is filtered by the internal RAKAA IT team and the secondary filtering is done by the Internet service provider Etisalat.
- RAKAA has an approved Filtering Policy that filters content related to age-appropriate groups: KG, G1-5, G6-9, G10-11 that is different from staff appropriate access.
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- RAKAA has a filtering and reporting system to report any breech in the firewalls or other relevant safeguards in place. The filtering system in place at RAKAA will prohibit and stop any searches for unauthorized concepts, pop-up that states site or access prohibited while auto logging the device used in the filtering system.

- RAKAA has appropriate security measures are in place to protect the users, equipment, workspaces, mobile/smart devices, RAKAA servers, firewalls, routers, wireless systems, from threats to technology used at RAKAA or possible accidental or intentional cyber threats to RAKAA school data and systems.
- RAKAA school infrastructure, equipment, filter and monitoring are protected using approved anti-virus software.
- The Visitor and Volunteer Use Agreement is in place to ensure that all users understand and are bound by the Acceptable Use Policy.
- RAKAA staff use follows the Acceptable Use Policy regarding the personal use of RAKAA network/systems both in and outside of school.
- RAKAA has a temporary/rental agreement for the use of RAKAA owned devices that follows the AUP as the devices are allowed to be used outside of school for their studies.
- RAKAA follows the Acceptable Use Policy regarding external removeable media hardware devices such as CDs/DVD/Memory Sticks.
- According to the personal data as noted in the policies- USBs and hard disks are not allowed. Teachers may use their own VPN but not when logged into the RAKAA learning network

Mobile Smart Devices, Technology, and (BYOD/BYOT)

Mobile smart technology devices will follow the Acceptable Use Policy, Mobile Policy, Child Protection Policy, Behaviour Policy, Cyber Bullying and Anti-Bullying Policies. Students may access RAKAA school network using their own personal device, or a school issued laptop or through the school ICT lab desktops. These devices will be to strengthen learning and widen the school's learning platform. The school organizes unique online safety training and understanding to all – students, teachers, volunteers, visitors, external service providers, MoE/MoL, and other users prior to accessing the RAKAA school network.

Students and parents must understand the safe and appropriate use of technology that is an integral part of their teaching and learning at RAKAA. Therefore, it is crucial for students to follow and have in place an Online Safety Education Program. RAKAA's OSE Program is developed following the above polices.

RAKAA follows the Acceptable Use Policy, Mobile Policy, Child Protection Policy, Behaviour Policy, Cyber Bullying and Anti-Bullying Policies while ensuring filtering and monitoring of use are in place. The following policy guidelines are in place:

- Personal devices include laptops, tablets, Chromebooks, mobile phones, and MacBooks.

- Students should not use mobile phones while in school. Students are prohibited from having mobile phones in class and must turn them in to a nominated adult each morning.
- Personal devices may only be used when a teacher has given permission and then can only be used for educational purposes. It should not be used for games, chat, or entertainment.
- Students may not use their personal devices during break times while waiting to be dismissed or on school transport.
- The use of mobile data to access the internet by any student thru VPN or hotspot is prohibited as this cannot be monitored or controlled through school's firewall.
- Students are not permitted to take photos or videos while in school on any of their personal devices without the express permission of a member of staff. No student is permitted to take photos of anyone else without their permission.
- Features on personal devices such as VPN, Hotspot, Airdrop or Bluetooth must be switched off when on-campus.
- Students must surrender their personal devices to any teacher or administrator upon request and grant this authorized personnel permission to examine their system to establish whether any policies have been violated. When personal device is brought to school students should not expect privacy as to any data saved in their devices.

Use of digital and video images

RAKAA has the responsibility to ensure safeguarding of our students, staff, and visitors in regard to capturing and publishing/posting digital images. While using digital images is current practices on social media, at RAKAA we follow Article 21 of the UAE Cyber Crime Law (Federal Law No. 5 of 2012), which states that "using a visual device to invade the privacy of a third party by capturing their picture or transferring, copying or keeping those pictures is a crime." (13) This is key to our online safety education at RAKAA. While technology advances so do digital images allowing people of all ages to access images – some educational or newsworthy with the correct permissions in place to post a picture, but most are not posted following UAE or International Cyber Imaging Laws. One of the key responsibilities of our Online Safety Policy and Online Safety Education as stated in the KPIs of the RAKAA eSIP is to educate our RAKAA Learning Community

and students using education and policies. We recognize the benefits of digital and video images for our students and greater learning community's learning of what is acceptable and aligned with UAE/MoE laws and RAKAA Policy as instant uploads of personal pictures of themselves or others have risks involved. Students, parents, staff, entire learning community need to be aware of laws and safeguards in place to protect their personal profiles and information. Using digital or video images irresponsibility have consequences that could be both illegal practice of uploading images without consent, cyberbullying, or give access to cyber predators or terrorism.

Training and understanding is part of our online safety education and policy to grow and develop an understanding of benefits, consequences, laws, digital citizenship, and best safeguarding self/other practices as once a digital images is uploaded into cyberspace of the Internet- those images remain forever. Therefore our school takes seriously the pastoral and safeguarding responsibility to educate RAKAA users of the inherent risks of the misuse of technology and digital images and will educate and implement RAKAA policies through delivery of curriculum, training sessions, awareness sessions, and development of student groups such as the ESafe School eSafe Student Ambassadors empowering and giving a voice to students to teach students and RAKAA learning community on how students learn and educate themselves and others about the benefits and consequences of following guidelines and the Acceptable Use and Online Safety Policies at our school. RAKAA will educate and inform all RAKAA users to reduce the risks of Unacceptable Use and raise awareness to the potential threats or risks to themselves, their families, the school, and their future selves following the RAKAA, UAE, MoE, and Child Protection laws (Wadeema's Law UAE).

Ensuring knowledge and understanding polices that are associated with digital image use, confidential personal information, rights and protection of others, consent for (sharing, posting, publishing) images. The internet firewalls and safety protections such as filtering, and monitoring are in place to track through data any attempts or unacceptable use/attempts to use technology. The school will follow strictly the policy and law as concerning posting to the school website or social media. The school will ensure that the policies for safeguarding the rights of student/parent/teacher/staff/others are understood and the Acceptable Use Policy and Consent to Photo and share on website or social media is in place for all in the RAKAA Learning community.

Any use of digital images or videos will be allowed as part of an educational objective or to validate/document actual learning outcomes for use in class- school website-inspections following receipt of understanding and consent from the parent/carer/student that follows the

policies of RAKAA and the UAE. The school will only used school owned devices and support teams to take types of digital images. However, a contracted service provider might be used for official class/student photos for parent purchase with the proper consent follow policy.

Data Protection

Data Protection is one of the priorities at RAKAA as a school and an education institution with which must request and maintain the integrity of private personal and confidential information. To ensure the highest level of protection for all within the RAKAA virtual and physical learning environments we follow UAE protocol to safeguard the personal data that must processed within the different departments of RAKAA using the UAE Data Protection Law: The Personal Data Protection Law of 2021 states:

"The law aims to enhance community protections from online crimes committed through the use of networks and information technology platforms, protecting public sector websites and databases, combatting the spread of rumors and 'fake news', safeguarding against electronic fraud and preserving personal privacy and rights." (15) RAKAA has developed a Data Policy designed to ensure the data collected from/about students, parents, teachers, staff, administration, employees, external providers and the personal information stored at RAKAA is dealt with correctly and securely. Our data policy applies to all information, regardless of how it is gathered, used, recorded, stored, or destroyed, and whether it is stored in paper or electronic forms.

By following the UAE Data Protection Law and RAKAA Data Protection Policy safeguarding, security, and integrity of personal confidential information. The policy is shared with the greater RAKAA through the Staff Handbook, Password Policy and Guidelines, Acceptable Use Policy, orientation, and training of policy for (student/parent/teacher), RAKAA website, and our eSafety SIP and digital curriculum.

To further ensure that data is protected RAKAA ensure the school has:

- scheduled reviews of our encrypted data protection systems and storage
- only transfers personal data to internal RAKAA departments as needed for processing in different departments
- collect and analyse data incident reports once per week to inform decisions
- secure authentications are in place for users accessing sensitive data including access to school systems offsite follow UAE data and personal data regulations and safeguards

- any personal information that needs disposed as redundant whether through staff leaving or a student withdrawing- all personal confidential data is disposed of properly as per our data protection and retention of data policy.
- Personal data is kept for a limited time as per best practices and is collected and disposed of properly in a safe secure organized manner
- Educates our students, parents, teachers, staff, and greater community about the UAE and RAKAA Data Protection Laws.

Communications

RAKAA is an educational institution that due to changes in teaching and learning styles as well as business models for schools in the post-pandemic world using technology for communication is a must. A wide range of rapidly developing communications technologies has the potential to enhance learning. To ensure that personal confidential information is kept confidential the school has firewalls to personal and school wide information. The greater RAKAA learning community receive training to understand the different types of communication that the students, parents, and staff will use and follow by the HR, Child Protection Officers, Online Safety Leader/Assistant OSL, IT, RAKAA Teachers and ESafe Student Ambassadors.

We consider using technology in teaching and learning as a integral part of teaching young people how to communicate and use technology safely.

Our school considers using technology a positive benefit and a must as we are living in the Technology Revolution and Era therefore, we need to be aware of the risks and take all precautions to safeguard our student/staff/school information while communicating on external sites. Training of staff and students on what is acceptable and follows the regulations of UAE Cyber Crimes Federal Law No. 5 of 2021, and the Online Safety and Acceptable policies use are key in educating our learning community about how to protect themselves and others as well as what is allowed and school and what is not. The reflection of our commitment to communication and integrity of use is found in the table below:

To ensure that our school is as safe as possible in the digital world we teach and work in RAKAA will post and hold awareness sessions with parents, students, teachers, and external visitors making them aware that:

- AUP is in place and RAKAA community accountable to actively reflect on what is acceptable use when using the internet or RAKAA network
- Only the RAKAA school email system will be used in school following AUP and UAUP
- External service providers will not be allowed to use their personal devices, take pictures, or access their personal hotspots or VPN services
- Reporting of unacceptable use or illegal practices are known and ways to report posted throughout school for students, parents, staff, visitors to report
- Students, parents, teachers are part of educational sessions addressing communication safety and acceptable use understanding potential threats, harm, or risks that unacceptable use of devices to communicate

- RAKAA virtual learning community are well knowledgeable about the UAE and RAKAA Policies that are in place for their present and future protection. Sucha s, but not limited to: Communication, DATA protection, Personal Data Protection, Password Protection, Digital protection laws., Acceptable Use, Unacceptable Use

Social Media – Protecting Professional Identity

Providing a safe physical and virtual learning environment is the responsibility of RAKAA. To ensure that our learning community is safeguarded against possible threats or dangers that are unfortunately a part of the fast-paced digital world that we live in. RAKAA takes this to heart as safety is our priority. To safeguard and protect our learning community from social media the school had the following steps in place to ensure a safe risk-free learning environment:

- Hiring teachers/staff who are highly qualified in their field, have had background checks/police clearances, reference in prior schools or workplaces contacted and confirmed that the potential employee does not have any indications that they might make-fun-of, bully, harass, degrade, or discriminate on the grounds of gender, nationality, race, or ability.
- Safety routines and guidelines that are embedded with the social media by:
    - Educating and training to ensure that personal private information is not shared or published.
    - Training to include safeguards that minimize potential risk to students, teachers, whole school and parents that inform and educate about:
        - Risks of social media (students/parents/staff)
        - Data protection and digital image protection (student/parents/staff)
        - Reporting infractions of misuse or illegal -who and how to report (student/parents/staff/volunteers/visitors)
        - Education about passwords safety, digital citizenship, responsibility of using the Internet safely
        - Incident reports, logs, filters in place to protect at the school
        - Legal actions for illegal acts- knowledge of Data Protection and sanctions for misuse of personal or professional data are in place
- Risk Assessments such as but not limited to:
    - Internal checking of firewalls, filters, and monitoring systems
    - External ‘Mock’ trials intentional challenge of firewalls
    - Check password security
    - Process of approvals in place prior to opening the schools’ social media accounts

RAKAA must diligently through regular review of the website that external use and access by the school or academic staff that there:

- That the school does not reference students or parents or staff
- Pictures of students/parents/teachers/staff/others are not posted without consent as per UAE Cyber Law of 2021

- Invasion of privacy does not happen as the as RAKAA must safeguard and protect the Whole School and keep confidential personal information private whether through applications for work or registration of students- information is not shared or able to access
- Students do not have access to teachers' personal matters or private access to personal social media platforms such as Instagram or Facebook or FaceTime
- RAKAA school matters and issues are private and are not discussed or imaged on social media
- IT assures that safeguards are in place to promote awareness and minimize the possibility of cyber-attack or theft of personal information through
- Acceptable use and unacceptable use are in place
- Reporting Channels are available and known (anonymously or open)

Personal social media accounts are not allowed at RAKAA to ensure the integrity of the school site. The school will safeguard itself with a disclaimer that any personal account used does not represent the thoughts nor values of RAKAA.

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- RAKAA permits reasonable and appropriate access to private social media sites to teachers

Monitoring of public social media

- The school will appoint a member of the Online Safety Group to monitor the social media engagement of part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

- RAKAA's use of social media for professional purposes are regularly checked by IT and the Online Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Unsuitable and inappropriate activities are more common in today's world than before as schools and the whole world are part of the fast-paced mechanism of data exchange freely throughout the world with the click of a mouse or button or even verbally using Siri or other avatars of search engines. That does not mean that all active searches or interactions using technology or unsuitable or inappropriate. This is an important distinction as all schools globally are now connected to the Web in some form or the other. Schools must actively use the internet to access technology for teaching and learning purposes. Therefore, safeguarding of access and exposure to possible

unsuitable and inappropriate for age website and links must be part of any good school's eSafe online protection policies.

It is our pastoral duty to safeguard our young people's age-appropriate content access. RAKAA's Online Safety Group and virtual and physical learning communities demand and expect the school to be the 'safe' learning environment it must be while ensuring age-appropriate learning material and engagement while accessing educational learning sites. The school is bond to educate the students, parents, teachers, staff, and community on what would be considered inappropriate, unsuitable, and unsafe content when accessing and using technology. Our school puts safeguards in place on devices and has policies in place to use as tools to educate what is acceptable and what is not. This is taught to KG-G12 as part of the eSafety Practices and Digital Citizenship. Activities such as digital safety week, student contests to create the best rap song that can teach other students to Avatar creation contest to be used as the 'spokes avatar' for RAKAA's eSafety learning. Further our school have come together through the OSG and Whole School as students, teachers, parents, staff, and community agree that the following would be inappropriate internet activity for use in school (onsite) or off campus (online).

Unsuitable and Inappropriate Activities have consequences which are identified in the RAKAA Unacceptable Use Policy with degrees and levels of sanctions that are supported by UAE Cyber Law, MoE Behaviour, and RAKAA Behaviour Policies. This list is updated and reviewed termly by the OSG and our eSafe School Student Ambassadors. RAKAA realizes and understands that this list is not exhaustive and must be a living practice in our pastoral and educational guidance to teach our students what is and what is not appropriate use when using digital technologies or when not using technology. We have the responsibility to develop intuitive safe digital citizens in our classes, so our students and the learning community recognize and understand why these sites and activities are harmful, inappropriate, unsuitable, and possibly illegal. ESafe digital education is the key.

Unsuitable and Inappropriate Sites
(not an exhaustive list)

- **Violence of all types**
- **Sexual or pornographic material**
- **Child abuse**
- **Human trafficking**
- **Cyberbullying -hazing**
- **Discrimination-of -race, abilities, gender, financial status, nationality**
- **Animal Cruelty**
- **Culturally inappropriate material**
- **Suicide/Death Challenges**
- **Teaching Hacking of Phishing**
- **Political Activism**
- **Hacking**
- **Phishing**
- **Plagiarism**

Responding to incidents of misuse

RAKAA has the responsibility to safeguard students and whole school information. Today's world is filled with instant access to sometimes restricted sites if someone with savvy technical skills can hack or phish for information to penetrate our school's protective eSafety barriers and firewalls. To this in as a contingency plan that 'what if' happened and there was an attempt to break into our RAKAA network system, our Online Safety Group has developed a Response Path for Incidents of misuse for data. Digital technologies within our system.

When an incident is flagged either through our monitoring system (i.e. automated filters, monitors, firewalls) or from our internal reporting system of unacceptable or misappropriate use of technology (online reporting using barcodes, QR Codes, incident reports, or direct reporting to teacher or OSL or OSLA or OSG or Child Protection Officer or to their parent who then reports to the school) there must be a path to investigate and determine why it happened technically (if there was a breach) or what steps need to be taken to ensure that the student knows and understand the depth of what they have done or tried to do when challenging they system to 'see' what would happen' in that what if situation.

Please find the Incident Misuse Response Path below:

Response Path for Incidents of Misuse of Data/Digital Technology at RAKAA	
Identification	1) Detection from our automated monitoring systems 2) Report to OSG (IT) what happened
Confer	3) With the OSL to evaluate the level of the breach or infrastructure issue. 4) Depending on level of technical infrastructure the IT team start their investigations using reporting and monitoring processes 5) Depending on level of data/digital protection or academic breach the OSL starts the OSG investigation process
Resolution-Technical	a) IT gathers facts about the incident and use automated processes to identify the issues and make adjustments to firewalls or updates to system protections as needed. b) Reports issues in the monitoring logs c) Depending on level and type. Possible to escalate to the police as per UAE Data Protection Law 2021
Resolution-Academic	a) OSL gather facts about the incident and uses internal OSG-Child Protection Officer, Behavior Committee (as per RAKAA student Behavior Policy and AUP) to discuss the incident. b) Behavior Committee determines the level of breach in the AUP, Data and Personal Information Protection, UAE Cyber Laws are all in place and are used to guide the decision. c) Student/Parent are met with, and incident discussed and reminded of AUP signed understanding and RAKAA Policies

Final-Technical	a) Findings of IT investigation are put into action b) Repairs/updates (if required) are put in place c) Higher standard of protections (if required) put in place
Final-Academic	a) Findings of academic investigation put into action b) Pledges/ contracts/training does as per policy c) Further steps (legal) as need are taken and the case is closed. But remains in student files.
External Threat (Parent or Other) to Data Protection	Police and legal authorities are called to assist or take over the investigation (As warranted) by the severity of the breach in Data Protection as per UAE Cyber Laws.

Illegal Incidents

Illegal Incidents are any incidents or infractions that are done at the school or off campus using the school's network that is considered illegal by RAKAA, the local or federal government, or an international law such as the Wadeema's Law of discrimination against ability levels. This could happen in a classroom or online. Another example of an illegal incident would be hacking into another student's or schools or other account off campus and stealing/accessing someone else's personal confidential data. Our responsibility to embedding in our teaching, learning, and role-modelling. Our eSafety curriculum, extra-curricular activities, student created 'lessons', celebrations of understanding and promoting eSafety and Digital Citizenship are ways that we at RAKAA are infusing good choices and raising awareness of the risks involved what can appear 'fun' or as a 'dare' can have long lasting personal impacts on the person who is engaged in illegal incidents and the innocent people who are victimized by illegal acts. RAKAA teaches students the what is acceptable and legal as well as what is considered unacceptable and illegal- such as cyber bullying or bullying, accessing blocked websites, plagiarism connected with the consequences of one's actions if the wrong choice is made. Education is again key, as through education students understand what is acceptable and what is not. Our students are taught to report incidents of suspected illegal or unacceptable use/access or behaviours. The reporting mechanism is to your teacher, anonymously through the incident report slip, using the bar code access, reporting to the OSL, OSLA, Principal, Child Protection Officer, Social Counsellor, their parent or other responsible adult. The school then investigates and follows the data protection, digital personal information protection, acceptable use and unacceptable use policies, as well as the RAKAA behaviour policy that is linked to the MoE Behaviour policies and UAE Cyber Laws.

Other incidents

RAKAA is aware that other incidents can require investigation and possible legal action that can be either cyber in nature or on campus. There are certain other incidents that require the involvement of the police or child protection agency depending on the type of incident.

All incidents follow procedures to safeguard at RAKAA when using technology:

1st Identify the computer that was used

2nd Remove from student user access to conduct investigation and monitoring procedure- depending on level of unacceptable use and type of illegal incident -the police may need to be involved

3rd OSG (IT) need to have access to investigate in detail

4th Capture the URL that was entered that the alleged incident of misuse or illegal access is noted and detailed in the incident report

5th Evidence such as screen shots or pictures or recordings may need to be collected to be used during the investigation of the machine.

6th Pictures or videos of children or child abuse cannot be printed or attached as proof of evidence to investigation into the incident. OSL and Child Protection Officer or Social Counsellor may need to be involved depending on type of incident and the safeguarding pastoral care required.

7th Once the investigation is complete the findings of the OSG and Behaviour Committee at RAKAA will determine the level of the offense and the next steps to take. RAKAA will follow the policy and procedures as listed in the Child Protection, Behaviour Policies, and guidelines for sanctions as per the MoE and UAE Cyber Law.

8th If the RAK or UAE Cyber police were required or social affairs or child welfare is required the documents gathered during the incident investigation will be handled by the police from that point on and confidentiality clauses signed by RAKAA staff that were involved with the investigation.

RAKAA Actions and Sanctions

RAKAA will follow the staff and student handbooks of policy to deal with incidents that involve inappropriate misuse and turn investigations that lead to the need for police intervention as listed above in the other incidents procedures. The RAKAA Student Behaviour Policy, Acceptable Use Policy, Unacceptable Use Policy, Cyber Bullying and Bullying Policies, Data Protection and Digital Personal and Data Protection Policies are supported and aligned to the UAE Cyber Laws and MoE Behaviour Policy and Procedures. RAKAA will use the incident reports that can be anonymous in nature if the person reporting (student or staff or parent or visitor) to investigate allegations of inappropriate misuse or behaviour following the above-mentioned policies that the levels of behaviour infraction and sanctions/consequences embedded within. RAKAA is not punitive…we are an educational institution that strives to create and raise awareness of making good life choices through education.

References:

1. Cyber laws - The Official Portal of the UAE Government
2. UAE: Up to Dh200,000 fine for creating fake e-mails, websites, online accounts (msn.com)
   Article (11) of the Federal Decree-Law No. 34 of 2021 on combatting rumours and cybercrimes, of the UAE Government
3. Emiri Decree No. 02 of 2018 amending the UAE Cybercrimes Law (Arabic)
4. Internet Access Management Regulatory Policy –TDRA
5. Digital Participation Policy | Digital Participation | Ministry of Energy and Infrastructure in UAE (moei.gov.ae)
6. Cabinet Resolution No (37) of 2014 on the Executive Regulations of Federal Law No (4) of 2012 concerning the Regulation of Competition | Ministry of Economy - UAE (moec.gov.ae)
7. Social Media Policy | Digital Participation | Ministry of Energy and Infrastructure in UAE (moei.gov.ae)
8. Intellectual property - The Official Portal of the UAE Government
9. Future skills for youth - The Official Portal of the UAE Government
10. ADSW Future Skills 2030.pdf
11. Student Behaviour Management Distance Learning 2020_English.pdf (moe.gov.ae)
12. Student code of conduct - The Official Portal of the UAE Government
13. UAE policy law using digital images - Search (bing.com)
14. Data protection laws - The Official Portal of the UAE Government
15. Personal Data Protection Law