RAK AA
RAS AL KHAIMAH AMERICAN ACADEMY
أكاديمية رأس الخيمة الأمريكية

e-Safety Policy

Policy date: January 2021

Review date: November 2021

Signatures:

_____ _____

Introduction

RAKAA eSafety policy is developed to maintain rigorous and effective eSafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimizing and managing any risks.
These eSafety practices aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Rationale

RAKAA has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition, RAKAA maintains a zero-tolerance policy to the bullying of students and staff and inappropriate use of technology.

Scope of the Policy

This policy encompasses the implementation to all stakeholders of the school which includes students, parents, staff, visitors, volunteers, carers, and other community members who have access and are users of school ICT technology, both on and off the school. This policy is an integral part of the Child Protection Policy as well as other related policies pertaining to safeguarding and regulation of the student's behavior on and off school site. This policy empowers members of the eSafety group to impose disciplinary penalties for inappropriate behaviour. This is applicable to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place in and out of the school by any of the stakeholders. Proper procedure/ protocol and sanctions will be applied by the school's eSafety group as indicated in our PBL (Positive Behavior Learning) process and in accordance with the MOE Code of Conduct/Discipline Policy.

Important terms used in this document:

a) The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies.
b) 'eSafety' refers to the safe and responsible use of the Internet and ICT equipment/devices.

c) The term 'ICT equipment/devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players),Gaming Consoles, and any other, similar, technologies as they come into use.

d) 'AUP' refers to Acceptable Use Policies issued to all stakeholders

E-Safety risks

It is no doubt that technology use and innovative ICT tools in school and at home can help raise the educational standard and foster student's achievement. However, the use of these new technologies can put danger and risk to young learners as well as adults in and outside the school.
Some of the dangers or risks they may face are as follows:

- Access to illegal, harmful, or inappropriate images or other content such as unsuitable video or internet games; downloading music or video files.
- Unauthorised access to, the loss of or the sharing of personal information

- Personal images or photos maybe shared or distributed without an individual's consent or knowledge
- Contact or communication with others or strangers in an inappropriate way
- Cyber-bullying
- Plagiarism and copyright breach
- Excessive use which may impact the social and emotional development as well as the learning of the students

Dissemination/Communication of the Policy

This policy is made accessible, communicated, and understood by all stakeholders through various ways such as:

- Posted on the School Website
- Available in the school network (Microsoft one drive, Microsoft Teams)
- Communicated thru Email for Staff, WhatsApp for parents, newsletter, Bi-weekly webinars conducted by the Principal
- Student and Staff Handbook
- Part of the Annual Induction of New and Returning Staff (includes support staff)
- Stated in the Acceptable Use Policies (AUPs) for students, parents, staff, visitors, community uses, governors, (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school and reissued if updated after annual review.
- AUPs are displayed in appropriate classrooms/corridors (not just in ICT corridors/classrooms)
- Reviews of this eSafety policy include input from staff, students, and other stakeholders, to ensure further engagement/ or involvement.

Roles and Responsibilities

The following outlines the eSafety roles and responsibilities expected from the members/stakeholders of the school:

Governing Board

- To be responsible for the approval of the eSafety and for reviewing the effectiveness of the policy through the annual reports, incident log and monitoring and auditing reports submitted by the eSafety Group validated and confirmed by the Senior Leadership Team.
- To ensure that appropriate funding is authorized for any eSafety solutions, relevant training to all staff and other activities as recommended by the Senior Leadership Team.
- To be actively involved in promoting eSafety information to parents and the wider community

Principal and Vice Principal

- To foster a culture of safeguarding where eSafety is fully integrated into whole school safeguarding
- To ensure that policies and procedures are followed by all staff
- To implement the procedures to be followed in case of a serious eSafety allegation being made against a member of the school community
- To ensure that the eSafety officer and group members receive proper training to enable them to carry-out their eSafety roles effectively and to train other staff

- To support the eSafety group in the implementation of the eSafety Policy and in their monitoring role
- To ensure that the Governing Board are regularly updated on the nature and effectiveness of the eSafety
- To ensure that there is a system in place to monitor and support the ICT Managers who carry out internal technical online safety procedures
- To liaise with the safeguarding leads on all online-safety issues which might arise and receive regular updates about school issues and broader policy and practice information
- To take overall responsibility for data management and information security ensuring that the School follows best practices in handling information
- To ensure that child protection is the priority to be considered in sharing data information
- To ensure that the school implements the effective use of appropriate ICT systems and services such as filtering, technical security, protected email system, cloud system in accordance with child-safety principle

eSafety Officer

- To develop an e-Safe culture throughout the school community as part of safeguarding, which is in line with national best practice recommendations
- To act as a named point of contact on all e-Safety issues and liaising with other members of staff as appropriate
- To audit and evaluate current practice to identify strengths and areas for improvement in collaboration with eSafety Group Members
- To lead an e-Safety team with input from all stakeholder group
- To embed e-Safety in staff training and CPD by ensuring that all members of staff receive up- to-date and appropriate e-Safety training (at least annually and as part of induction) which sets- out clear boundaries for safe and professional online conduct.
- To ensure that there is an age and ability appropriate e-Safety curriculum that is embedded, progressive, flexible, and relevant which engages children's' interest and promotes their ability to use technology responsibly and to keep themselves and others safe online. Incorporating eSafety in our Digital Citizenship will serve this purpose.
- To ensure that e-Safety is promoted to parents/or guardians and the wider community through a variety of channels and approaches-such as professional development workshops, sharing circular and policy updates
- To ensure there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support
- To liase with the ICT managers in ensuring that age-appropriate filtering is in place, which is actively and regularly monitored
- To ensure that appropriate risk assessments are undertaken termly regarding the safe use of technology, including ensuring the safe and responsible use of devices
- To collaborate with the IT team for data protection and data security and specific related policies to ensure that practice is in line with legislation
- To maintain an e-Safety incident/action log to record incidents and actions taken
- To liaise with the local entity such as MOE and or other local and national bodies as appropriate

- To review and update e-Safety policies, Acceptable Use Policies and other procedures on a regular basis (at least annually for inclusion in Student Handbooks), with stakeholder input and ensuring that eSafety is integrated with other appropriate school policies and procedures-Cyber bullying, Acceptable Use Policy, Distance Learning Policy expectations
- To monitor and report on e-Safety issues to the school management team, Governing Body and other agencies as appropriate
- To preserve a high level of confidentiality in respect to the personal information of the stakeholders
- To maintain and build good working relationship with the team and colleagues in order to carry out the eSafety policies and practices effectively
- To report regularly to Senior Leadership Team

ICT Managers

- To ensure tight security of the school's technical infrastructure and make certain that it is not open to misuse and/or malicious attack
- To ensure that the school meets required eSafety technical requirements
- To ensure that all network systems including remote access, Virtual Learning Environment (VLE), internet and email are regularly monitored so that log reporting can be done immediately for any misuse and/or prevention of misuse
- To ensure that all stakeholders are aware of the guidelines and procedures that need to be followed in case an eSafety incident occurs.
- To enforce strict password protection policy for all users which includes parents and visitors before accessing the school network and device and if possible, a regular change of password should be done for stronger security
- To implement filtering and technical security policy and keep it updated on a regular basis
- To receive reports of eSafety incidents and keep a log of incidents for appropriate action, follow-up and future eSafety development
- To provide advice and eSafety training for all stakeholders
- To ensure that the school's ICT system and network are secured and protected from virus and malware and safety mechanisms are updated regularly
- To be responsible in blocking access to potentially dangerous sites to prevent the downloading of the dangerous files
- To maintain an up-to-date documentation of eSafety guidelines, protocols, and procedures, and ensure that all policies are communicated to all stakeholders and sign agreements are obtained

Teaching and Support Staff

- To ensure that they have a clear understanding of eSafety Policy and other related policies, procedures, guidelines, and practices and have signed an agreement to all the policies
- To adhere to all the terms and conditions stipulated in the eSafety policy
- To ensure that they know who is the eSafety Officer and other Safeguarding lead members for reporting incidents and for further guidance in the implementation of the eSafety policy
- To report any misuse or suspected misuse to the eSafety Group for investigation and

appropriate action and sanction

- To ensure that all digital communications with students, parents and other members of the community should be on a professional level and done using the official school network systems
- To ensure that during lessons, students are guided to sites that are suitable for use and strictly enforced students' understanding of research skills and to avoid plagiarism and acknowledged and adhere to copyright rules.
- To enhance students' awareness about the eSafety policy, guidelines and protocols pertaining to mobile phones, ICT devices, camera and monitor their use and constantly reminding them about the terms and conditions stated in the eSafety policy
- To ensure that any incidents of cyber bullying are reported and or actioned appropriately in accordance with the Student Behavior Policy, Anti bullying Policy and Discipline Policy
- To be actively involved in all eSafety training conducted by the school
- To be a model of responsible and professional behaviour in their own use of technology and social media in and outside school campus upholding the trust and reputation of the school community.

Designated Safeguarding Lead Team (Head of Student Support/Counsellor/Social worker, Head of Sections, Quality Assurance Team, ICT Managers)

The responsibilities of this team which are set based on our Child Protection Policy and other safeguarding policies are as follows:

- To ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- To ensure that any incident of cyber bullying is logged, and appropriate measures and sanctions have been taken in line with Anti-bullying Policy, Student Behavior Policy and Discipline Policy
- To liase with other external agencies if necessary, to safeguard children
- To stay updated on the latest trends of online safety for better safeguarding
- To promote an awareness of online safety to all the members of the community and help them develop their commitment and support to the full implementation of eSafety Policy
- **E-Safety Rules to be displayed next to all PCs in school and stay safe**
    - **S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.
    - **M**eeting up with someone you have met online can be dangerous.
    - **I**nformation online can be untrue, biased or just inaccurate. Someone online may not be telling the truth about who they are – they may not be a 'friend'
    - **L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.
    - **E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Students

- To be a responsible user of the school digital technology systems in accordance with their signed agreement of the Student Acceptable Use Policy (AUP) and other related eSafety policies and guidelines
- To develop a deep understanding of the research skills, plagiarism, and copyright guidelines
- To ensure that all material being accessed on the internet is appropriate.
- To seek clarification about accessing websites or other sources of information where they may be unsure of content.
- To ensure that communications with other students, staff members and members of outside community do not harass, vilify, or attack personally other individuals. This includes, but is not limited to, written words and the posting of images.
- To report to parent/guardians or teachers any inappropriate communication through ICT equipment devices which are used in or out of school time
- To recognize the importance of exercising good eSafety practices which are implemented on and off school site
- To ensure that they know the PBL (Positive Behavior Learning) process in reporting for any misuse and/or abuse, cyber bullying, misconduct/ inappropriate behavior and that they are aware of the consequences of their bad actions.
- To understand the benefits, opportunities as well as risks and dangers of online technology and they know to whom they should report to if they encounter any problem

Parents

- To ensure that their children understand the need to use the internet, mobile devices, and any other technology in an appropriate way.
- To support the school in encouraging responsible communication using ICT equipment and devices. Provide Online tools which control your kids' access to adult material and help protect them from Internet predators.
- To explain the internet use permission for their child/Children.
- To take the opportunity to attend eSafety training conducted by the school, parent's meeting for any eSafety information and issues
- To support the school in providing good eSafety practices and adheres to all the policies related to safeguarding and safety

Visitor/Community Users

- They will be made aware of the eSafety policy if they are given an access or allowed to use the school's ICT system. They are expected to agree to the terms and conditions on the acceptable use.

eSafety Education and Curriculum: e-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- eSafety Induction at the beginning of the school year for all staff and students (new and returning)

- A planned eSafety curriculum that is an integral part of the ICT, Digital Citizenship, and other lessons and that should be regularly reassessed
- Key eSafety messages are reinforced in various subject lessons, assemblies, webinars, and other school activities
- Students are constantly reminded to be critically vigilant of the materials/ content that they access online. Likewise, they are guided to validate the accuracy of the information
- Students are taught to acknowledge and to respect copyright of the source of information/materials used on the internet
- Students are helped to understand the terms and conditions in the Student Acceptable Use Policy (AUP)
- Staff are continuously trained to make them role models of good eSafety practices and develop digital resilience
- Parents will continuously be provided of eSafety training and information campaign through webinars, newsletter, website, email, whatsApp to enhance a deeper awareness of the eSafety practices to monitor and guide their children
- The Governing Board is encouraged to initiate and/or participate in eSafety training/awareness session to enhance their understanding about eSafety practices

eSafety Prevention Duty of Care

All staff of RAKAA are encouraged to be vigilant and persistent in inculcating to the minds of the students the eSafety best practices. As part of their pastoral care, they must ensure that students:

- Develop the courage to talk openly to their parents and/or guardians about what they see online and tell them if anyone asks for personal information
- Commit themselves to follow the eSafety rules in school and family rules when playing online games
- Understand the importance of being cautious when sharing personal information online that includes real name, address, phone number, school name, password, and other private information
- Commit to follow the following eSafety ethics:
  - Post only information or photo that you feel comfortable sharing with the whole world
  - Never use the ICT technology in spreading gossip, bully or hurt other's reputation and feelings
- Identify the security tools available on most computers/devices to protect their information and protect their devices from virus and malwares
- Enhance awareness about the online potential unreliable influences about their beliefs and ideas and report immediately the incident to a trusted adult in the school

Technical – infrastructure/network, filtering and monitoring

RAKAA is responsible for ensuring that the school infrastructure/network is safe and secure, and the policies created for this purpose are implemented. Likewise, it is expected that the members of the eSafety group will carry out their responsibilities effectively.

The school ICT technical system is managed by the eSafety safeguarding lead (ICT Managers) and ensure that the school meets the technical requirements stipulated in the Acceptable Use Policies.

- Regular reviews and audits of the safety and security of the ICT technical system
- Ensure that the location of the servers, wireless systems and cabling are properly secured, and the physical access is restricted

- All users are given access rights to the school ICT technical system and devices
  - Users' internet access is filtered
  - Users are aware that the ICT Managers regularly monitor and record the activity of the users and that it is clearly stated in the AUP agreement
- There is an appropriate system for reporting of any actual/potential technical incident/security breach
- Appropriate security measures are done to protect the servers, firewalls, routers, mobile devices, wireless system, computers, etc. from malicious attacks or threats to the security of the school ICT system and data
- An up-to-date virus software is installed to protect the school infrastructure and individual workstations
- A provision of temporary access for the school ICT technical system is provided to the visitors or community users after agreeing to the AUP's terms and conditions
- Only encrypted or secured personal data can be sent online or taken off the school

Use of Digital and Video Images

RAKAA staff is expected to inform and educate the students when using digital and video image and the risk associated with the taking, sharing, publishing, and distributing their own images on the social networking sites. Provisions for the use of digital and video images are as follows:

- Ensure that students are appropriately dressed when their photos are being taken and they are not doing activities that may harm other individuals and disrepute the school
- Allow staff to take digital or video images for educational purpose and must follow the school policies pertaining to sharing, distribution and publication of those images
- Parents and student's permission will be sought first before taking student's image/photo, use, share, distribute and publish it on the school website, newsletter and other promotional literature

Data Protection

RAKAA is committed to protect all stakeholders' personal data. All staff are guided in the proper safekeeping of personal data to minimize misuse or its loss. Transferring of data is done through encryption and secured password. Staff are advised to minimize the use of USB stick or any other removable media for protection from virus and malwares.

Social Media

All stakeholders are required to sign an agreement that they have read, fully understood, and guided by the terms and conditions stipulated in the Social Media Policy. To further enhance the implementation of this policy, the school ensures that appropriate measures are undertaken such as:

- Staff training about acceptable use, social media risks, checking of setting,
- Clear reporting and guidance, procedure, and sanctions
- Risk Assessment
- Ethical behavior expectation from staff such as: no reference should be made in social media to students, parents, and school staff; online discussion of personal matters relating to the member of the school community is prohibited
- Regular checking of the security setting of the social media profiles to minimize risk of loss of information

Response Protocol for eSafety Concerns and Incidents

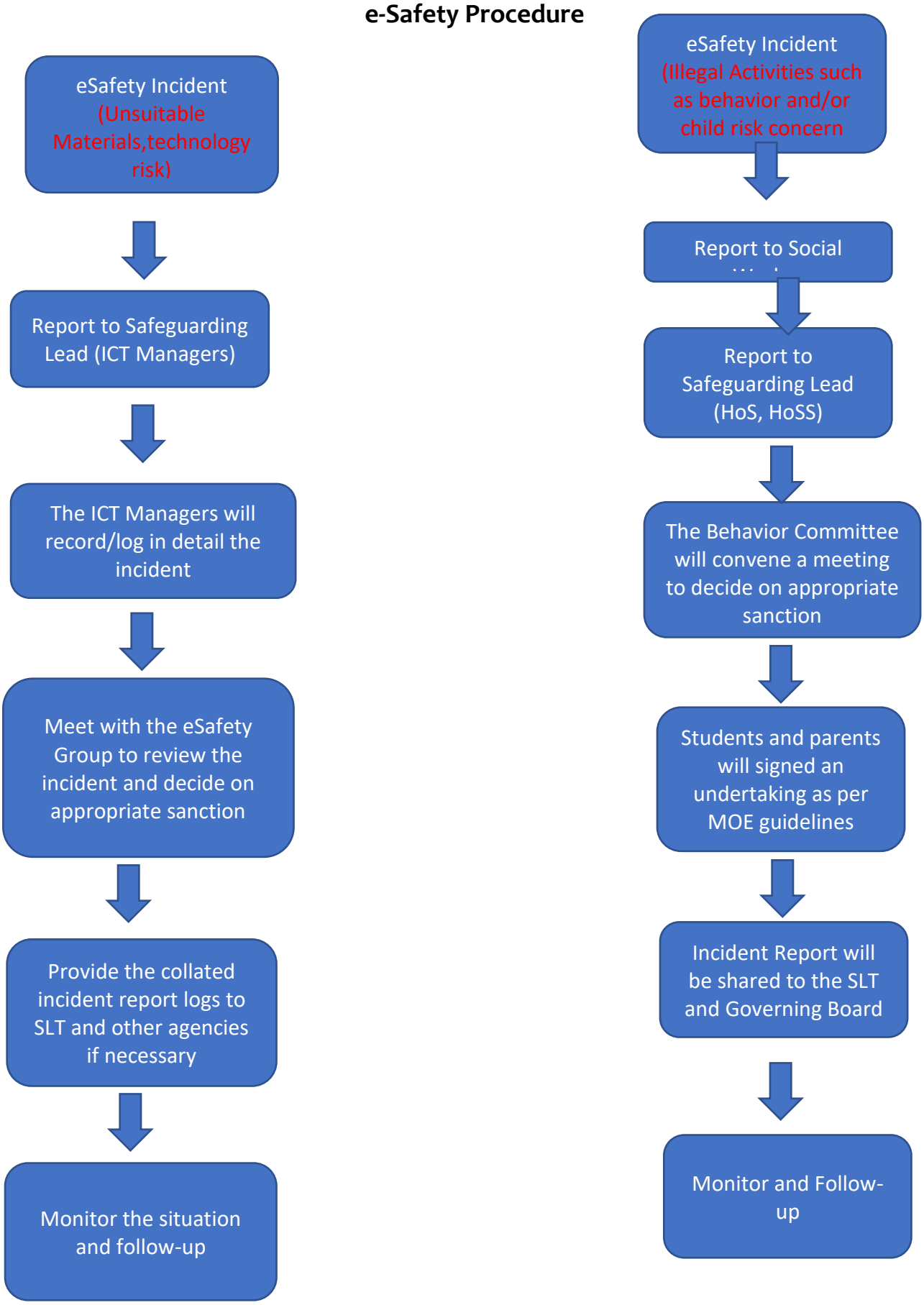
Though RAKAA has put its best effort to provide a safe physical and online environment, it is inevitable that on some occasions, misuse of the internet and other ICT technologies may still occur. RAKAA ensures that appropriate strategies, procedures, and protocols are to be followed by all stakeholders to address eSafety concerns ands incidents. A detailed procedure for dealing with online safety related to cyber bullying, inappropriate behaviour such as cheating, violence and aggression is outlined in the Child Protection Procedure and Positive Behavior Learning (PBL).

Other eSafety incidents and illegal activities that the students may commit are as follows:

- Copying information from the internet without acknowledging the source (plagiarism and copyright violation
- Downloading materials irrelevant to their studies (breach to the school's acceptable use policy)
- Misconduct related to student log in such as using other's password
- Using their device to send annoying message to someone or taking unauthorized photo

To address these eSafety incidents, the following procedure (flow chart) alongside with the Child Protection Procedure and Positive Behavior Learning (PBL) will be applied:

e-Safety Procedure



Linked Policies and cross-references

Child Protection Policy, Student Behavior Policy, Anti bullying Policy, Discipline Policy, Health and Safety Policy, Data Protection Policy, Social Media Policy, Student Email Communication Policy, Distance Learning Policy, Password Policy and Guidelines, Policy for Use of Removable Media, Student Personal Laptop Acceptable Use Policy, Cyber Safety Policy, Job Description of eSafety Officer, Staff Email Communication Policy, Child Protection Procedure, Positive Behavior Learning (PBL), eSafety Development Plan, eSafety Group Terms of Reference

Schedule for Development / Monitoring / Review

Approval of the Updated eSafety Policy	School board, March 2021
Monitoring of the implementation of eSafety Policy	SLT
The Governing Board will receive the report of the implementation of the eSafety Policy as well as monitoring and auditing report as recorded by the eSafety group	Annually
Review of the eSafety Policy	Annually
Monitoring of the Impact of the eSafety Policy thru	Log incident report Survey feedback from stakeholders-termly
Contact Agency for serious incidents	MOE Child Protection Unit
	Police Department

Created: 2018 as Cyber Safety Policy by Ms. Nathaalie
Updated: January,2021 by Dr. Maria
Updated: November 2021 by Ms. Farhat Riffat