مدرسة رمسيس الإنجليزية الخاصة
Ramsis English Private School

RAMSIS ENGLISH PRIVATE SCHOOL

Online Safety Policy

2021-2022

Updated By	Latest Publish Date
E-safety Team	December 2021

This e-safety policy was approved by the Leadership team on:	September 2020
The implementation of this e-safety policy will be monitored by the:	Online Safety Team
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: December,2022	December,2020
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Paula Payne (Principal)

The school will monitor the impact of the policy using: (delete / add as relevant)

- Logs of reported incidents
- Surveys of reported incidents:
  - Students
  - Parents / Guardians
  - Staff

Introduction

At REPS we are committed safeguarding our students through prevention, protection and support. We believe that everyone in the school community has the right to learn and to teach in a supportive and caringenvironment without the fear of being bullied.

We are committed to helping all members of the school community to benefit from information and communication technology, while understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

The school recognizes that any bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

Purpose

As a school, it is our duty of care alongside that of staff/parents/careers and other members of thecommunity to protect our children and young people from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this policy is to outline what measures we take to ensure that pupils can work inan e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriatemanner.

This E-Safety policy enables our school to create a safe learning environment that:

- protects children from harm
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for all on acceptable use of the internet.

Aims

- to use technology safely and respectfully
- to identify a range of ways to report concerns about content or contact
- to show how to keep personal information private
- to recognize acceptable/unacceptable behavior
- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting REPS students at school and at home.

- Putting policies and procedures in place to help prevent incidents of cyber-bullying within\or outside the school community.
- Having effective and clear measures to deal with and monitor cases of any online incident such as cyber-bullying.

Scope to the policy:

This policy applies to all members of the school community (including staff, pupils, parents / guardians, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. At RAMSIS ENGLISH PRIVATE SCHOOL we understand the responsibility to educate our pupils all related e-Safety issues; teaching them the appropriate behaviors and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Information and Communications Technology (ICT) covers a wide range of resources including; web- based and mobile learning. It is also important to recognize the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Online Learning Platforms and Virtual

Learning Environments Email and Instant

Messaging

- Podcasting

Videos

Broadcasting

- Downloading from the
- internet Gaming
- Mobile/Smart phones with text, video and/or web functionality

Other mobile devices with web functionality

E-Safety Roles & Responsibilities

As Online Safety is an important aspect of strategic leadership within the school, the Admin, the Head of department teachers and teachers have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The school community have an understanding of the Online Safety issues in relation to local andnational guidelines and advice.

Our school will endeavor to ensure the e-safety of all its members. It will use education, technology, accountability and responsibility as the key ways to achieve this. Within our school, all members of staff and pupils are responsible for Online safety.

Responsibilities for each group include:

Students

Students are responsible for ensuring that:

- Behave responsibly and appropriately when using communication technology including the internet and online platforms.
- Student must follow the Behavior policy.
- Abide by the guidelines given to them regarding reporting abuse, misuse or access to inappropriate content.
- They know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- Do not respond to cyberbullying. Take evidence (pictures or print outs of emails, messages, pictures or videos sent).

Teaching Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school Online Safety policy and practices.
- They report any suspected misuse or problem to the Online Safety coordinator or the Head of department.
- All digital communications with students/parents/careers should be on a professional level and only carried out using official school systems; School Website or the school official emails.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed)

and implement current policies with regard to these devices.

- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use.
- Motivate students in displaying positive behavior online.
- Attend courses which are offered by the school regarding E-safety Education.
- Apply what they have learned in the courses.
- Provide the school with the completion Certificates of the described courses.

IT Department

School IT department is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.

  - That the school meets required e-safety technical requirements
  - That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.

- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the E- safety officer/ Principal for investigation/action/sanction.

E-Safety Leader\coordinator– Mayada Nabel

- Leads the e-safety committee
- Leads on e-safety issues
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- send referral to the social worker to Inform parents when a warning is given
- Informing the social worker to deduct the behavior marks and record it.
- Coordinate with social workers on all behavior cases.
- Promotes an awareness and commitment to e-safeguarding throughout the Designated Child Protection Lead or school social worker
- Ensures that online safety education is embedded across the curriculum
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident;
- To ensure that an online safety incident is logged as a safeguarding incident and is kept up to date;
- Facilitates training and advice for all staff; Oversee any pupil surveys / pupil feedback on online safety issues

Social worker; Ayat

Social worker is responsible for ensuring that:

- she promotes awareness on all forms of bullying for students, parents, and staff members.
- she runs national anti-bullying week program.
- she maintains and review anti-bullying and cyberbullying policy
- she maintains records of behavior management incidents.
- she follows REPS policies and MOE behavior policy when dealing with e-safety/cyberbullying cases.

- she maintains records of each cyberbullying case, or any related incident.

Parents

Parents are responsible for ensuring that:

- Children are monitored when they are online, especially during online learning phase.
- They are warned of the negative side of communication technology.
- Children are instructed to report any concerns to them or the school admin, Online Safety Leader or social worker.
- They help their child act with self-confidence.
- Parents/guardians are required to make a decision as to whether they consent to images of their child being taken/used on the school website. Attached to the new admissions forms.
- Parents are encouraged to look at the school's policies.
- Parents receive an e-safety bulletin attached to the student behavior policy at least once per term.
- Parents are expected to ensure that their kids do not carry devices or electronic goods of any form without the express written approval of the Supervisor concerned.
- Parents must at all times demonstrate restraint and respect for the members of the school community, including all students and personnel.
- Parents must not breach confidentiality, defame or make threats to any person in the school community. Instances of proven and intentional breach of the above will result in the matter being referred to the MOE.

ICT teacher:

- Ensure that all pupils are given clear guidance on the use of technology safely and positivelyboth in school and beyond including how to manage their personal data and how to report abuse and bullying online.
- provide annual training for parents/careers on online safety and the positive use oftechnology
- Ensure that the school's Acceptable Use Policy, and guidelines are implemented by Staff and Students who are using digital devices such as the school Computers in the ICT Lab.
- provide annual training for staff on the above policies and procedures
- provide annual training for staff on online safety

- plan and deliver a curriculum on online safety in computing lessons which builds resilience in pupils to protect themselves and others online.
- plan a curriculum and support staff in delivering a curriculum on online safety which builds resilience in pupils to protect themselves and others online.

Online 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:

- A planned e-safety curriculum should be provided as part of Computing / Well-being, PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned program of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

  Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit and don’t depend on the filtering system only.

internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach E-Safety.

- Students are aware of the impact of online bullying and know how to seek help if these issues affect them. Students are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e., parent/guardian, teacher/trusted member of staff, or Police by using smart APPS like My Community is Safe

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Introducing the e-Safety policy to STUDENTS

- E-Safety rules are displayed in the ICT suite and discussed with the students at the start of each lesson. All staff are aware that at least one dedicated e-safety lesson must be taught each month and at relevant points throughout e.g. during ICT lessons//anti-bullying week/Safer Internet Day.
- STUDENTS will be informed that network and Internet use will be monitored**.**

STUDENTS have signed Acceptable Use

- Acknowledgment**.** staff have signed

  Acceptable Use Acknowledgment**.**

Parents have signed Acceptable Use Acknowledgment**.**

Education – Parents / Careers

any parents and careers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s on-line behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

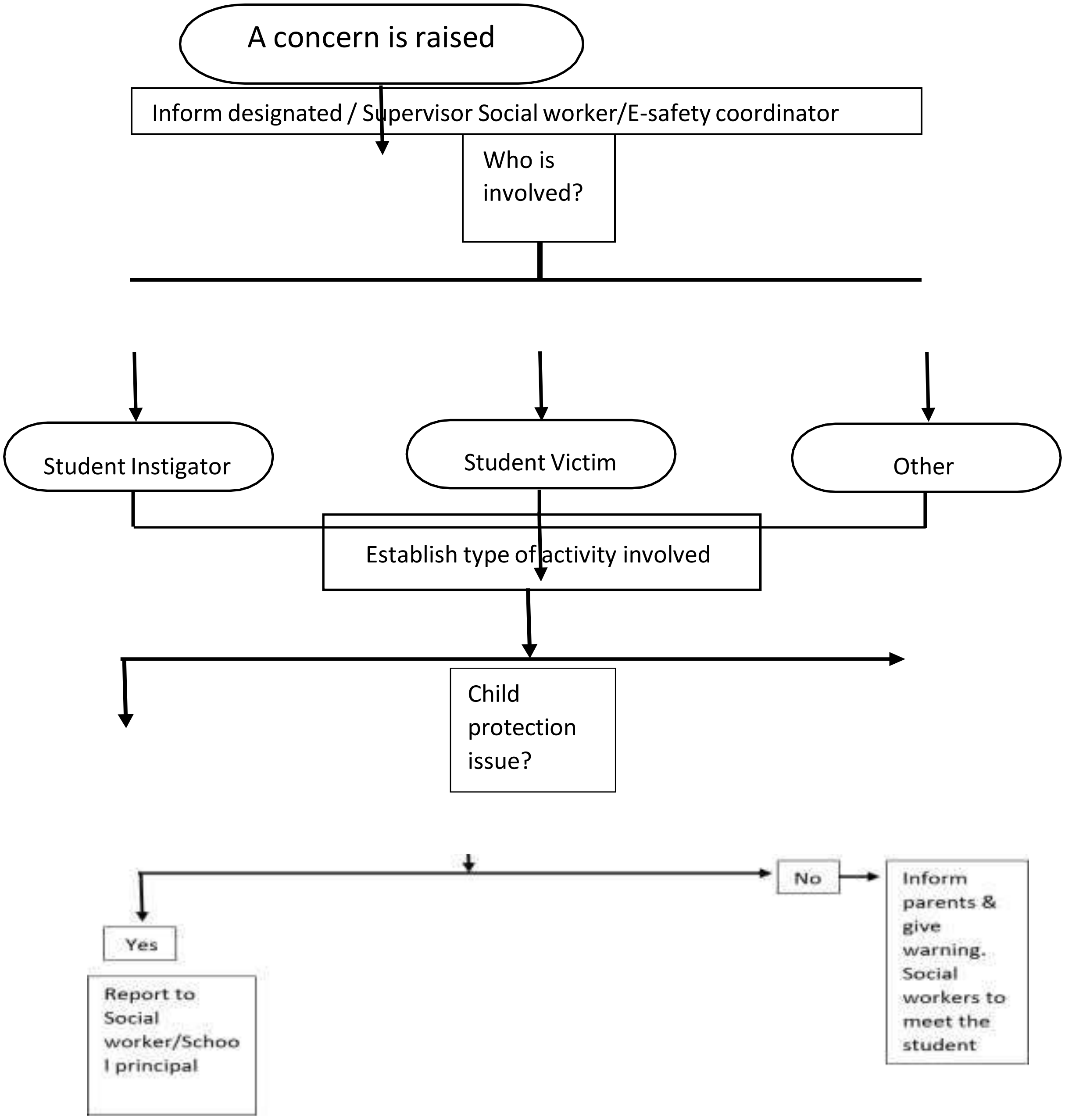
the school will therefore seek to provide information and awareness to

parents and caregivers through: Curriculum activities
Letters, newsletters, website
Parents meetings / sessions
High profile events / campaigns e.g.
Safer Internet Day Reference to the
relevant web sites / publications

practices and Procedures

the school will encourage safe use of IT, emphasizing, for example, the importance of password security and the need to log out of accounts.

the school will promote the message that asking for help is the right thing to do. All members of the school community will refer to the flowchart below to report any e-safety concern/ cyberbullying.


A concern is raised
Inform designated / Supervisor Social worker/E-safety coordinator
Who is involved?
Student Instigator
Student Victim
Other
Establish type of activity involved
Child protection issue?
Yes
Report to Social worker/School principal
No
Inform parents & give warning. Social workers to meet the student

investigation

The nature of any investigation will depend on the circumstances. **The E-safety team** which consists of the Principal, the Academic Team, the Head of Section, Social Worker, and ICT teacher will be involved in all E-safety & cyberbullying cases. The investigation may include:

- A review of evidence and advice to preserve it, for example by recording or saving orprinting (e.g. phone messages, texts, emails, website pages, screenshots of online learning platforms).
- Efforts to identify the perpetrator, which may include looking at the media, systems andsites used.
- Speaking to witnesses who may have useful information.
- Requesting a student to reveal a message or other phone content or confiscating aphone (Staff do not have the authority to search the contents of a phone\Phones are not allowed in the school).

Working with the perpetrator

Work with the perpetrator and determine sanctions on an individual basis, with the intention of:

- Helping the person harmed to feel safe again and be assured that the bullying will stop
- Holding the perpetrator to account, so they recognize the harm caused and do notrepeat the behavior
- Helping bullies to recognize the consequences of their actions and facilitating change inthe attitude and behavior.

handling e-Safety complaints

- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher;
    - Any suspected online risk or infringement is reported to Online Safety Coordinator that day
    - Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator
- ⌜ Any complaint about staff misuse must be referred to the Principal Assistant.
- ⌜ Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures.
- ⌜ Students and parents will be informed of the complaint’s procedure.

Note: Always report bullying incidents. Not doing that allows the bully to continue. That's not good for the victims, for those who witness the incidents or for the bully, who may needhelp to change their behavior.

Technology Platforms.
The teachers will use appropriate platforms for each year/grade level groups for effectivedistance\Face-to Face learning. Some of the key platforms being used are: -

KG

Zoom – to facilitate online Lessons, assemblies, events, discussions, meetings and sharing of resources. For more information please visit https://support.zoom.us/hc/en-usor please see Zoom Guide in our website or Telegram Channel.

Class Dojo - enables teachers to share content, distribute quizzes, assignments, and managecommunication with students, colleagues, and parents.

For more information, please visit https://classdojo.zendesk.com/hc/en-us/categories/200185365-For-parents

Grade 1-6

1. Zoom – to facilitate online Lessons, assemblies, events, discussions, meetings and sharing of resources. For more information, please visit https://support.zoom.us/hc/en-usor please see Zoom Guide in our website or Telegram Channel.

2. Class Dojo - enables teachers to share content, distribute quizzes, assignments, andmanage communication with students, colleagues, and parents
3. Nearpod – Student engagement platform where teacher can create presentations thatcan contain quizzes, polls, videos, images, drawing-boards, web content.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safeand secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meetsrecommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical accessrestricted
- All users will have clearly defined access rights to school technical systems and devices
- The IT Department is responsible for ensuring that software license logs are accurate and upto date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users

    - An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
    - Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
    - Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Ramsis English Private School ensures that:

- Students will be made aware of acceptable and unacceptable Internet use.
- Students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy ofinformation.
- Students will be educated about the effective use of the Internet.
- Students will be taught how to evaluate Internet content by ICT teachers.

- Students will be taught how to report unpleasant Internet content to their classteacher, supervisor.
- The school Internet access is designed expressly for student use and includesfiltering appropriate to the needs of our students.
- Where students are allowed to freely search the internet, staff should be vigilantin monitoring the content of the websites they visit.
- The use of Internet-derived materials by students and staff complies withcopyright law.
- All students and staff understand the importance of password security and theneed to log out of accounts.

Social networking and personal publishing:

The school provides the following measures to ensure reasonable steps are in place tominimize risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; dataprotection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Personal opinions should not be attributed to the school

The school has a duty of care to provide a safe learning environment for all students and staff and will ensure the following:

- Blocking student access to social media sites within school boundaries
- Educating students about why they must not reveal their personal details orthose of others, or arrange to meet anyone from an online site
- Educating both students and staff as to why they should not engage in onlinediscussion revealing personal matters relating to any members of the schoolcommunity.
- Educating both students and staff about ensuring all technological equipment isalways password/PIN protected
- Informing staff not to accept invitations from students or parents/guardians onsocial media.
- Informing staff about regularly checking their security settings on personal socialmedia profiles to minimize risk of access of personal information

E-Safety skills development for staff

- All members of staff receive regular information and training on E-Safetyissues through Online courses or the coordinator\ICT teacher at staff meetings.

- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and knowwhat to do in the event of misuse of technology by any member of the school community.
- All members of staff incorporate e-Safety activities and awareness at the startof every Week of the term and during the Online Safety Events.

Published content and the school web site

The contact details on the school website are the school address, e-mail andtelephone number. Staff or student’s personal information is not published. Head of department teachers along with the IT technical support will take overall editorial responsibility and ensure that content is accurate and appropriate.

Social networking and personal publishing

- The school blocks access to social networking sites.
- **Students and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g., Facebook) for primary aged students.**
- Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our students are asked to report any incidents of bullying to the class teacher or to the E-safety coordinator.

  Our students are asked to report any incidents of bullying\cyberbullying\ or any online safety issue to the secret box if they don’t want to mention their name.

School staff are advised not to add children, or parents as ‘friends’ on their social media accounts.

Managing emerging technologies

- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Students are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school are sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.

Protecting personal data

The school will use information about students to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school.

Password Security

- Adult users are provided with an individual network username and password,email address which they are encouraged to change periodically.
- All members of staff are aware of their individual responsibilities to protect thesecurity and confidentiality of the school network.
- All staff must sign that they have received an official e-mails passwords.
- Any information downloaded must be respectful of copyright, property rightsand privacy.

Please see REPS Password Security Policy

The school will hold personal information on its systems for as long as individual members of staff remain at the school and remove it in theevent of staff leaving or until it is no longer required for the legitimatefunction of the school.

- Each teacher has the right to view personal information that the schoolholds and to have any inaccuracies corrected.

Publishing student’s images and work

- Written permission from parents or guardians will be obtained before photographs of students are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child’s circumstances where consent could be an issue.
- Parents/ guardians may withdraw permission, in writing, at any time.
- Photographs that include students will be selected carefully and will notenable individual students to be clearly identified.
- Student’s full names will not be used anywhere on the school website,particularly in association with photographs.
- Student’s work can only be published by outside agencies with thepermission of the student and parents.

Photographs taken by parents/ guardians for personal use

In the event of parents/ guardians wanting to take photographs for their own personaluse, the school will demonstrate our protective ethos by announcing that photographstaken are for private retention and not for publication in any manner, including use onpersonal websites, e.g., School performances and assemblies etc.

Please see the school’s Admission Form

Parent awareness and training:

The school offers advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensurethat principles of online safety behavior are made clear;
- Information leaflets; in school website;
- Suggestions for safe Internet use at home;
- Provision of information about national support sites for parents.
- provides induction for parents which includes online safety;
- runs a rolling program of online safety advice, guidance and training for parents.

Ramsis English Private School Server and Website:

- **REPS server is provided by Hostek services.**
- **REPS server is protected by network-level and server-level firewalls and antivirus software. The firewall is configured in a manner to block all incoming connections except to ports that you specifically have opened in your Firewall Management tool within the Windows Control Panel.**

- **Server software is configured to automatically update and can be updated on-demand with a support ticket as needed.**

- **REPS current backup plan is "7 Local Nightly Backups". This means that the entire server is backed up on a nightly basis and that seven retention points (a week) are kept on a secure backup server within the same data center. These backups can only be accessed by members of HOSTEK team.**

HOSTEK Terms and Conditions:
https://hostek.com/tos

Access to school facilities is regarded as a privilege and not a right. Access may be denied if a user breaches the conditions of Acceptable use

1. Notify an adult immediately, if by accident, you encounter materials that violatethis Acceptable Use Policy.
2. Be prepared to be held accountable for your actions and for the loss of privilegesif you breach this Policy.
3. Do not share your password with another person.
4. Log out of the network whenever you leave a computer unattended.

Support

- □ Academic issues – Any academic issues should be firstly raised to the teacher/subject teacher. Should you require any further clarification, thenplease contact the HOD responsible for your child's grade level.
- □ IT/Technical/E-Safety Issues – Please contact the IT coordinator for any issues arising with log ins, software or other technical elements during thedistance learning period for E-Safety.

Writing and reviewing the e-Safety policy

This policy (for staff, students, visitors and Parents), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, home-school agreements, Behavior, Child Protection, and other policies including filtering, password security, emails.

We encourage parents to set up filtering on their home internet. To learn how to dothis for the major providers of internet please click the text below.

- □ Setting up internet filtering and parental controls
- □ https://support.google.com/googleplay/answer/1075738?hl=en
- □ https://parentalcontrol.eset.com/?stscheck=NQAyADgAMQBiADgAMAAwAC0AMwBmADEAOAAtADQANABiADkALQA4AGQAMQBhAC0ANAAxADMAMwA2ADUANAA4ADAAZAA0ADIA

We also suggest parents visit the TELEGRAM CHANNEL link below for up-to-date information on privacy settings, cyber bullying, how to protect your personal information,gaming, and all the information needed to be safe while using Internet.

- https://t.me/Esafetychannelramsisschool

Monitoring and reporting of online safety incidents

Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records arereviewed/audited and reported to the school's principal.

Parents / careers are specifically informed of online safety incidents involving youngpeople for whom they are responsible.

We will contact the Police if one of our staff or pupils receives online communicationthat we consider is particularly disturbing or breaks the law. we will immediately refer any suspected illegal material to the appropriate authorities – Police, Digital Wellbeing Council, and CPU.

Enforcement

Reporting Violations

A reporting system has been added to the school website so you can easily report anyE-safety incident. All users can use it.

Users who believe they have witnessed or been a victim of a violation of this Policy should notify or file a complaint in the attached link or visit the website; www.ramsisschoolrak.com and click **report now** as follows: student Users should report suspected violations to the E-safety coordinator through the secret box on the website or to their class teacher ; staff users should report suspected violations to the E-safety coordinator and to the HOD's; guest Users should report violations to InformationTechnology Services.

Cyber safety and digital security are serious issues in the UAE. Read how the UAE isprotecting its citizens and residents in this field and reinforcing digital trust.

Report cybercrimes online

You can report cybercrimes online through the following channels:

- □ My community is safe App:
  Community participation in providing community protection from cybercrime by communicating through this application with the Federal Bureau of Investigation. As this service provides the public with the opportunity to report any crime or suspicion that occurs through social networking sites that violates public security or threatens community security, public morals, public order, or cases that have anegative impact on public opinion.
  https://appadvice.com/app/d9-85-d8-ac-d8-aa-d9-85-d8-b9-d9-8a-d8-a2-d9-85- d9-86/1380618945
- □ the eCrime website
- □ Dubai Police's website

□ the ‘My Safe Society’ app launched by the UAE’s federal Public prosecution (theapp is available on iTunes or Google Play)

You can also report cybercrimes to the nearest police station in your area, or call 999for help.

Related links:

- Reporting prohibited content to the Internet Service Providers in UAE ;

https://www.tra.gov.ae/en/about-tra/information-and-egovernment-sector/internet- guidelines/details.aspx#description

Child Protection Unit (CPU):

CPU@moe.gov.ae

- Cyber safety and digital security in UAE LAW:

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and- digital-security

- Digital wellbeing support line
http://wam.ae/ar/details/1395302823342

80091 is the UAE Digital Wellbeing Support Line (content in Arabic), the first initiative of the Digital Wellbeing Council. The support line provides professional advice from dedicated experts for all members of the family on practical daily situations we face in the digital world.

- Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights, also known as Wadeema's Law

states: The telecommunications companies and internet service providers shall notify the competent authorities or the concerned entities of any child pornography materials being circulated through the social media sites and on the Internet and shall provide necessary information and data on the persons, entities or sites that circulate such material or intend to mislead the children.

- The Dubai Data Law (Law No. 26 of 2015 on the Organization of Dubai Data Publication and Sharing) aims for data protection and privacy of all individuals including that of children.

https://www.smartdubai.ae/ResourcePackages/Theme/assets/dist/docs/Data%20Disse mination%20and%20Exchange%20in%20the%20Emirate%20of%20 Dubai%20Law_20 15.pdf

Violations of This Policy

Violations of the above rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's AUP, E-safety, and Behavior Management policies. Violations of this Policy will be addressed under the policies and rules regarding students, school and staff. The violations described in this Policy range from minor to extremely serious; even a minor offense may be treated severely depending on the circumstances. Certain violations may also be subject to prosecution under local laws.

Please see Cyber safety and digital security in UAE LAW:

https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and- digital-security

Related Policies

- REPS Student Behavior Management Policy for Distance Learning
- REPS Safeguarding and Child Protection Policy
- REPS Acceptable Use Policy
- REPS Password Security Policy
- REPS Filtering Policy
- REPS Managing Mobile Technologies Policy
- REPS Emails Policy
- REPS Distance Learning Policy

The policy effectiveness will be checked annually. E-SAFETY TEAM will do this during reviews conducted between the e-Safety Coordinator, Designated Child Protection Coordinator. Ongoing incidents will be reported to the concerned team.

Declaration

Please only sign if you have fully read the REPS Online Safety Policy. By signing the acceptance form you are agreeing that you have fully understood the REPS Online Safety Policy.

I hereby confirm that I have read and fully understood the terms and conditions document attached and will strictly follow the REPS Online Safety Policy

Date: Signature:

Reviewed: OCTOBER,2020. Reviewed: DECEMBER,2020.
Reviewed: December,2021