مدرسة رمسيس الإنجليزية الخاصة

Ramsis English Private School

Ramsis English Private School

ACCEPTABLE USE POLICY 2021-2022

Acknowledgment:

We in RAMSIS ENGLISH PRIVATE SCHOOL are pleased to be able to offer our students, staff and guests access to computer technology, including access to the Internet, certain online services, and the RAMSIS ENGLISH PRIVATE SCHOOL information technology network. We are dedicated to access and support of appropriate technology which unlocks our potential and connects us locally and globally. We envision a learning environment where technology is a part of us, not apart from us.

We believe that the tremendous value of technology and the information technology network as an educational resource far outweighs the potential risks. We will leverage existing and emerging technology as a means to learn and thrive in the 21st Century and prepare our students for success toward their goals in the competitive global, electronic age. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education. However, if parents feel they do not want their child to have Internet access, then they will be responsible for informing their child's teachers, in writing, before the end of the second week of school or they can mention their intentions in the admission form which is signed by the parents before joining the school.

Computers and networks provide access to resources as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly.

To ensure that our students become proficient in the information and communication technologies (ICT) competencies essential for success in a 21st century learning environment, RAMSIS ENGLISH PRIVATE SCHOOL provide a variety of resources in support of our instructional and administrative programs. Staff may also, at times, use their own personal information and communication technologies for educational purposes. Therefore, it is incumbent upon all members of the school community to use technology responsibly, ethically and respectful for the work of others.

Access to ICT resources is a privilege and not a right. To ensure that ICT resources remain available in working order, RAMSIS ENGLISH PRIVATE SCHOOL has established an Acceptable Use Policy (AUP) and Guidelines which define the procedures and parameters under which these resources may be used by all staff, students, volunteers, and service providers. To accommodate future needs and circumstances, the AUP, procedures and guidelines related to ICT resources will be regularly reviewed, updated and distributed.

Users must respect the rights of other users; respect the integrity of the system and related physical resources; and observe all relevant laws, regulations, and contractual obligations. Use of computers by students and access by students to computer networks and to the Internet are services made available only to further the educational mission of **Ramsis English Private School**. In order to be granted these access privileges and to retain them, students must abide by the guidelines set forth in the "Acceptable Use of the Internet and other Electronic Communication Systems for Students" policy and these regulations at all times when they use **Ramsis English Private School** systems. These computer systems are expensive to purchase, install and maintain. As the property of the school these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, access to the computer systems is a privilege, and not a right. **Ramsis English Private School** students may use the school's computers and network systems provided to them at school but they should:

- **Abide by the Acceptable Use Policy**
- **Sign an "Acceptable Internet Use Agreement"**

- **Obtain the signature of a parent/guardian (for receiving and reading AUP)**

The school's information technology resources, including website Account, Dojo codes and Internet access, are provided for educational purposes. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher, supervisor, online safety coordinator or director to help decide if a use is appropriate. Adherence to the following policy is necessary for continued access to the school's technological resources:

Rationale:

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of IT-based technologies;
- Safeguard and protect the children and staff of our school;
- Assist school staff working with children to work safely and responsibly with the internet and other IT and communication technologies and to monitor their own standards and practice;
- Set clear expectations of behavior and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community;
- Have clear structures to deal with online abuse such as online bullying which are cross referenced with other school policies;
- Ensure that all members of the school community are aware that unlawful or unsafe behavior is unacceptable and that, where appropriate, disciplinary or legal action will be taken;

Users must respect and protect the privacy of others by:

1. Using only assigned accounts.
2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.
3. Refraining from distributing private information about others or themselves.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all school Internet filters and posted network security practices.
2. Reporting security risks or violations to a teacher or network administrator or anonymously by reporting to the secret box.
3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.
4. Conserving, protecting, and sharing these resources with other users.
5. Notifying a staff member or administrator of computer or network malfunctions.

Users must respect and protect the intellectual property of others by:

1. Following copyright laws (not making illegal copies of files, documents, and videos).
2. Citing sources when using others' work (not plagiarizing).

Users must respect and practice the principles of community by:

1. Communicating only in ways that are kind and respectful.
2. Reporting threatening or discomforting materials to a teacher or administrator.
3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct or honor code (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
5. Not using the resources to further other acts that are criminal or violate the school's code of conduct or honor code.
6. Avoiding spam, chain letters, or other mass unsolicited mailings.
7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

Users may, if in accord with the policy above:

1. Communicate electronically via tools such as email, chat, text, or videoconferencing.
2. Install or download software, if also in conformity with laws and licenses.
3. Use the resources for any educational purpose during school hours.

New employees and students:

So that all users remain informed of our expectations and appropriate usage of ICT resources, the E-safety team will: 1) ensure all new students and staff receive trainings and tools during the enrollment and hiring process, as well as on-going training in their safe, responsible, and effective use; and 2) provide orientation annually for students and staff on ICT resources and the school AUP and Online Safety Policy.

In order to initiate and maintain access to ICT resources, all students, staff, visitors, consultants, service providers, and visitors must submit annually a signed Acceptable Use Agreement (detailed below). Violations of the AUP are deemed as violations of school behavioral expectations and policies.

The monitor of the ICT resources, reserves the right to monitor and review the use of these ICT resources and will do so as needed to ensure that the systems are being used for school-related educational purposes and to maximize utilization of the systems for such. It is important that all users and parents understand this and recognize that monitoring access,

- maximizes the safety and security of people and resources by supporting a positive learning and work environment safe from harassment, intimidation or
- discourages breaches of confidentiality, copyright infringements and inappropriate file downloads and print requests

- promotes appropriate internet access, electronic communication messages (such as email, blogs, chats and discussion forums).

Usage Guidelines - All technologies provided by the school are intended for education purposes. All students are expected to use good judgment and to follow these guidelines as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access and Security - RAMSIS ENGLISH PRIVATE SCHOOL provides students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with filtering system regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. **Students who wish to use the Internet must have a signed acceptable use policy on file each school year.** Students must keep in mind their use of technology will be supervised/monitored by teachers, staff members, parents and computer programs and filters. This includes before, during, and after school hours. **Students are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web.**

Computers and networks provide access to resources as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly.

Users must respect the rights of other users; respect the integrity of the system and related physical resources; and observe all relevant laws, regulations, and contractual obligations. Use of computers by students and access by students to computer networks and to the Internet are services made available only to further the educational mission of RAMSIS ENGLISH PRIVATE SCHOOL. In order to be granted these access privileges and to retain them, students must abide by the guidelines set forth in the "Acceptable Use of the Internet and other Electronic Communication Systems for Students" policy and these regulations at all times when they use RAMSIS ENGLISH PRIVATE SCHOOL systems. These computer systems are expensive to purchase, install and maintain. As the property of the school these computer systems must be carefully handled and their integrity preserved for the benefit of all. Therefore, access to the computer systems is a privilege, and not a right.

Student Behavior:

Students are expected to use all computer equipment, both hardware and software and network access to pursue intellectual activities, to seek resources, to access libraries and for other types of learning activities. They will learn new things and can share their new found knowledge with classmates, teachers, parents and global learning partners. For the safety of all involved, caution must be exercised.

Because RAMSIS ENGLISH PRIVATE SCHOOL s' network is used as part of a school activity, **the policy on student behavior applies to network activity**. **Therefore, the Acceptable Use Policy is an extension of the school behavior Management Policy**, **General Behavioral Policy, Online Safety Policy, Filtering policy, and Child Protection and Safeguarding Policy**. These rules apply to vandalism of computer equipment, unauthorized access to information, computer piracy, hacking, tampering with hardware and software, bullying and harassment.

- **Please see Ramsis's Students Behaviour Management Policy.**
- **Please see Ramsis's Students General Behaviour Policy.**
- **Please see Ramsis's Online Safety Policy.**
- **Please see Ramsis's Filtering Policy.**
- **Please see Ramsis's Child Protection and Safeguarding Policy.**

Parent awareness and training:

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

- Introduction of the Acceptable Use Agreements to new parents, to ensure that 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.

Monitoring

It is expected that students will comply with RAMSIS ENGLISH PRIVATE SCHOOL standards and will act in a responsible and legal manner at all times, in accordance with the school standards, and country laws. It is important that students and parents understand that the school, as the monitor of the computer systems, intends to monitor and review the use of these computer systems in an effort to ensure that users engage only in appropriate uses.The monitor and review process includes oversight of Internet site access, review of email and of document downloading and printing.

Therefore, all users must be aware that *they should not have any reasonable expectation of personal privacy in the use of these computer systems.*

Filtering system:

Filtering should be viewed as only one of a number of techniques used to manage students' access to the Internet and to encourage acceptable usage. Filtering should not be viewed as a foolproof approach to preventing access to material considered inappropriate or harmful to minors.

Filtering should be used in conjunction with:

- Educating students concerning the dangers of inappropriate material on the Internet;

- Using recognized Internet gateways as a searching tool and/or homepage for students, in order to facilitate access to appropriate material
- Using the school's "Acceptable Use" agreement
- Using behavior management practices for which Internet access privileges can be earned or lost.
- Appropriate supervision, both in person and/or electronically.

Internet Safety:

Students are expected to conduct themselves in an appropriate manner at all times when they use or interact with any of RAMSIS ENGLISH PRIVATE SCHOOL 's hardware and software resources. This includes, but is not limited to, interaction with school's computers, email communication, web browsing software, or even usage of one's own personal hardware over a district network connection.

To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including interacting with other individuals on social networking websites, gaming, instant messaging, video messaging, chat rooms, and cyber-bullying awareness, plagiarism, and response.

- **Initiatives on cyber security**
    - **Salim- an online cyber security advisor**

The UAE Computer Emergency Response Team (aeCERT) jointly with Aqdar, launched the initiative Salim, an online cyber security advisor, with the slogan 'Towards a safe cyber culture'.

The goal of this initiative is to spread knowledge about cyber safety to the entire community and have a generation that has integrated knowledge about information security and is mindful when conducting activities online.

Public may report any cybersecurity incidents through aeCERT.

- **UAE Ambassadors for electronic security**

This initiative from TRA aims to train top UAE students to serve as ambassadors in promoting and spreading cyber security awareness across the UAE. Read about other cyber security initiatives in the UAE.

- **Cyber blackmailing**

In 2016, the Dubai Police's Al Ameen service in cooperation with the UAE's Telecommunications Regulatory Authority (TRA) organized a cyber-blackmail awareness campaign. The campaign aims to protect victims from blackmailing by chasing all criminals in all parts of the world, in addition to issuing requests to the Interpol to hunt these criminals wherever they are. Read more on cyber blackmailing and how to stay safe.

- **Cyber C3**

Cyber C3 is an initiative that aims to develop ‘digital citizens’ who are able to benefit from online participation while taking responsibility for self-protection and the potential consequences of their online behavior. Cyber-citizenship goes beyond safety and risk. It calls for positive engagement in the online environment.

- **Cyber citizenship**

Cyber C3 is designed to produce digitally literate and responsible UAE citizens by certifying knowledge and understanding in the following areas:

- Cyber access
- Cyber literate
- Cyber rule
- Cyber safety
- Cyber interaction and collaboration
- Cyber enterprise
- Cyber care
- Cyber accountability.

The programme targets students from grades 9 to 12, college and university students, professionals, parents and family foundations. The UAE cybercrime laws are embedded in the curriculum to foster the understanding of these laws through local case studies.

Read these resources from Cyber C3:

- Top internet safety tips for parents
- Cyberbullying
- e-Security and eCommerce
- Digital reputation.

Supervision and Monitoring

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees; its technician and E-safety coordinator may monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school’s information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access.

This policy is an important part of the Leadership improvement plan to maintain a safe, civil, respectful, and inclusive learning community and shall be implemented in conjunction with comprehensive training of students, staff and volunteers.

The school will provide students with strategies aimed at preventing harassment, intimidation, and bullying. In its efforts to train students, the school will seek partnerships with families, law enforcement, and other community agencies.

Classroom blogs, student e-mail, podcasts, Google Apps accounts, online curriculum software/websites or other Web interactive tools must follow all established Internet safety guidelines. Staff and students using blogs, podcasts or other web tools for educational purposes are expected to act safely. Students using such tools agree to not share their username or password with anyone other than their teachers and parents and treat blog spaces and online spaces, or discussion forums, as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog. Users who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences consistent with the school's behavior management policies.

Enforcement

Reporting Violations

It is the school's policy that no student should be required to tolerate such treatment, regardless of the identity of the sender of the message.

A reporting system has been added to the school website so you can easily report any E-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 can report violations to the online Safety Coordinator or anonymously through the **secret box**.

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

Report cybercrimes online

You can report cybercrimes online through the following channels:

- the eCrime website
- Dubai Police's website

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

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

- 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%20Dissemination%20and%20Exchange%20in%20the%20Emirate%20of%20Dubai%20Law_2015.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-,Behavior Management, Online Safety, Child Protection, and Filtering 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

Penalties for Violations(Unacceptable Use)

The range of possible sanctions as a result of violations of this Policy includes, but is not limited to, the following:

- Loss of Electronic Resources privileges;
- Disconnection from the school's Network;
- Disciplinary sanctions as outlined in the School's E-safety policy, Behavior Management Policy, and AUP.
- If necessary; Referral to other authorities for civil litigation and criminal prosecution under applicable civil or criminal laws.
- Discipline of employees up to and including termination of employment.

Communication:

How the policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staffroom/ classrooms/corridors;
- Policy to be part of school induction pack for new staff;
- Policy to be a part of the new employees' contracts;
- Regular updates via email, staff meetings or bulletins and training on online safety for all staff.
- Acceptable use agreements discussed with pupils at the start of each year;
- Acceptable use agreements to be issued to whole school community, usually on entry to the school;
- Acceptable use agreements to be held in pupil and personnel files.

Any parent or student inquiry regarding any decision relative to Ramsis's Acceptable Use Policy and/or these administrative regulations should be directed to the E-safety coordinator.

Related Policies

- REPS Student Behavior Management Policy for Distance Learning
- REPS Child Protection and safeguarding Policy
- REPS Online Safety Policy

- REPS Password Security Policy
- REPS Filtering Policy
- REPS Managing Mobile Technologies Policy
- REPS Emails Policy
- REPS Distance Learning Policy
- REPS Complaints Policy
-

Declaration

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

I hereby confirm that I have read and fully understood the terms and conditions document attached and will strictly follow the REPS Acceptable Use Policy.

Date:

Signature: