INDIAN SCHOOL

RAS AL KHAIMAH

Acceptable Usage Policy

This policy & procedures are reviewed annually to ensure compliance with current regulations.

Approved/ Reviewed by	
Policy Lead	Jubairiya Sageer
Role	Personal & Social Development Coordinator
Date of Publication	08-04-2022
Date of First review	10-04-2023
Date of Second review	10-04-2024
Date of Third review	10-04-2025
Date of Fourth review	06-04-2026
Version	5.0
Date of next review	01-04-2027
Signature	

ICT Acceptable Use Policy forStudents

What is this policy: This Acceptable Use Policy outlines theguidelines and behaviors that all users are expected to follow while using the school's digital resources on the school campus

Aims:

- The aim of the Acceptable Use Policy is to ensure that all users within the school are aware of the different risks and hazards of the IT infrastructure usage, and useit sensibly and safely only for the purpose of teaching, learning and other related uses.
- All users should be free of any fear of cyberbullying by anyone known or unknown.
- All users should be able to recognize cyberbullying and to be able to recognize theproper ways to deal with it effectively

Scope:

- Acceptable use of the IT related infrastructure by any user within the school premises.
- Anti-cyber bullying.
- Improving the awareness level of digital devices usage.

Principles of Acceptable and Safe Internet Use:

- The School places ownership on all IT resources within the school.
- The School has the right to monitor and supervise all data transactions that are happening within theschool's network.
- The school has the right to block any content that would be considered as unsuitable or have anyeffect on the school, staff, students or society.
- Unauthorized installation of software is not permissible at all
- The school will provide an Acceptable Use Policy for any guest who needs to access the schoolcomputer system or internet on school grounds.
- The school will ensure that appropriate levels of supervision exist when external organisations makeuse of the internet and ICT equipment within school.

Acceptable uses of the School's internet systems for students are:

- Using the internet for educational purposes only, such as research, information gathering, sharingrequired files, assignments and any other related use.
- Using the internet to do online tasks that are only approved or advised by the teacher.
- To do projects or presentation for school's lessons.

- Responsible access for social websites for educational purposes only and under the teacher's supervision.
- Always, keep using an appropriate language in all digital communications, such as emails, socialwebsites or messages.
- Making sure that all user devices are taken care of

Acceptable uses of the School's internet systems for Staff are:

- Are committed to the responsible and effective use on the internet and other digital resources.
- Use the internet only for school related purposes.
- Ensure that there is no unauthorized use of the internet or other digital resources within the school.
- Promoting the good use of the internet to other school parties
- Provide a proper support to the students which is related to their social development through E-Learning and real-life experiences
- Share good practices involving different skills across the school.

Roles and responsibilities for schools E-Safety:1- School leadership team will:

- Provide educational guidelines about appropriate online behaviors, including awareness about interactions and communication with others through different online platforms.
- Raising the awareness level about cyber bullying and appropriate techniques in dealing with it.
- Ensuring the safety and security of students while using any digital resource.

2- Students will:

- Read, understand and adhere to the school pupil Acceptable Use Policy.
- Help and support the school in the creation of e-safeguarding policies and practices and to adhereto any policies and practices the school creates.
- know and understand the use of mobile phones, digital cameras and handheld device, use of mobilephones and cyberbullying related policies.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Take responsibility for each other's safe and responsible use of technology in school and at home,including judging the risks posed by the personal technology owned and used outside school.
- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and to befully aware of the incident-reporting mechanisms that exists within school.
- Discuss safeguarding issues with family and friends in an open and honest way.

- Ensure they will not share or divulge any personal information about themselves, their family members, or other people through any digital communication medium.

Never share any images of others without permission.

- Not to arrange any appointments with strangers or people they met online.
- To inform immediately any trusted adult about any suspicion or uncomfortable content they mightreceive online.
- To get in touch immediately with the relevant staff in case of facing a cyberbullying matter.
- Avoid trying to access any website that has adult, inappropriate or restricted content.
- Not to damage any of the school's digital resources including both hardware and software
- Help in increasing the awareness level across school and other students about the acceptable use ofthe digital resources.

3- Staff will:

- Spread the knowledge about the proper use of digital resources.
- Increase the level of awareness about cyberbullying and provide guidelines to others about how toreact and whom to contact when occurs.
- Make sure that there is no misuse of the digital resources to the best of their knowledge.
- Increase the awareness level about the pros and cons of different social media platforms when applicable.
- Support the collaborative habits using different digital resources.

4- Child Protection Officer: ● To understand the issues surrounding the sharing ofpersonal or sensitive information.

- To understand the dangers regarding student access to inappropriate online contact with adults andstrangers.
- To be aware of potential or actual incidents involving grooming of young children
- To be aware of and understand cyberbullying and the use of social media for this purpose.

5- Parents will:

- Monitor and guide their children and make them aware about the acceptable use of the internet andother different digital resources.
- Help and support the school in promoting e-safeguarding.
- Enforce the family and society acceptable values
- Got involved with their children in regular discussions regarding different challenges they might facethrough surfing the internet.
- Make sure that their children are aware enough about the acceptable use and the consequences ofbreaking rules.
- Taking full responsibility for monitoring their children's use of internet and other digital resourcesoutside

the school.

- Conduct regular discussions with their children to make sure that they are not subjected to any formof cyberbullying and to increase their awareness level about the topic.
- Cooperate with the school and inform about any misuse is reported or discovered.
- Ask the school to help in case of any cyberbullying or other related incidents.

6- Visitors will:

Visitors should be aware that the use of the Internet through the School's WiFi is monitored for safeguarding, and conduct purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose,including the investigation of welfare concerns, concerns about extremism, and the protection of others.

- I agree that connecting my own personal digital device to the school WiFi network willresult in the School's monitoring:
  - The name of my device;
  - The date and time the device was used on the network;
  - The IP address of my device.

7- Contractors will:

If Contractors is given Access to Internet in connection with the Services, Contractors shallnot tamper with, compromise, or circumvent any security or audit measures used in connection with the systems. All Contractors connectivity to internet and all attempts at the same shall only be through security gateways/firewalls and only through approved security procedures. Contractors shall not Access, and shall not permit unauthorized persons or entities to Access, or networks that contain school Data without express writtenauthorization, and any such actual or attempted Access must be consistent with any such authorization.

8- General :

The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact the Network Administrator

Violations of this policy:

School is dedicated to complying with the UAE Federal law 'The Prevention of Information TechnologyCrimes' which provide clear guidelines regarding what is permissible and what is punishable in the usage of the digital resources and the internet space.

Consequences for Device Misuse

The following consequences will be applied progressively based on the severity and repetition of misuse incidents:

1. **Warning and Counselling:** For first-time or minor offenses, the student will receive a warning and mandatory counselling sessions to address the behaviour and its impact.
2. **Parental Involvement:** Parents/guardians will be notified and involved in meetings to discuss the incident and collaborate on behaviour improvement strategies.
3. **Loss of Device Privileges:** Temporary or permanent loss of the privilege to use school devices, depending on the severity of the misuse.
4. **Detention:** The student may be assigned detention during breaks or after school hours.
5. **Behavioural Contract:** The student may be required to sign a behavioural contract outlining expected behaviour changes and consequences for further incidents.
6. **In-School Suspension:** The student may be placed in in-school suspension, where they will complete their work in a supervised setting away from their peers.
7. **Out-of-School Suspension:** For severe or repeated incidents, the student may be suspended from school for a specified period.
8. **Restitution:** In cases of damage or theft, the student may be required to pay for repairs or replacement of the device.
9. **Legal Action:** In cases where device misuse constitutes a criminal offense, the school may report the incident to the appropriate legal authorities.

Promotion of this policy:

This policy will be promoted through circulars, workshops and school's communication channels forall staff and parents. Involving the E-Safe school policies within different class sessions and initiaterelated competitions would support the awareness raising in this and other related topics.

Monitoring and Evaluation:

All Phases of the School will have a leader in charge leading the implementation of this policyAll teachers and Support staff would play the role in monitoring the
usage in every class and within School. The IT department would be supporting in the evaluationand the information collection on a termly basis. A report from each phase would be generated and collectively evaluated by the School leadership team.

Any areas of concerns would be identified from the number of reported cases, the investigationprocedures, actions taken and subsequent next steps as well as the information collected fromthe students involved. These will be evaluated to provide guidelines for a plan of action to improve the policy and its deployment. This policy would be reviewed on an annual basis after evaluating its effectiveness

INDIAN SCHOOL, RAS AL KHAIMAH

Acceptable Use Agreement for FoundationPhase children (1 to 5)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer equipment.
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do orif I think I have done something wrong..
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use acomputer.

Signed (child):……

Signed (parent): ……..

INDIAN SCHOOL, RAS AL KHAIMAH

Acceptable Use Agreement for Key StageTwo children (6 to 12)

I understand that while I am a member of Indian School, RAK I must use technology in aresponsible way.

For my own personal safety:

- I understand that my use of technology will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upsetwhen I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the School:

- I will not try to access anything illegal
- I will not download anything that I do not have the right to use.
- I will only use my personal device if I have permission and use it within theagreed rules
- I will not deliberately bypass any systems designed to keep the school safer.
- I will tell a responsible person if I find any damage or faults with technology,however this may have happened.
- I will not attempt to install programmes of any type on the devices belongingto the school, without permission.

I understand that I am responsible for my actions and the consequences. I have read andunderstood the above and agree to follow these guidelines:

Name ***Signature*** ***Date***

INDIAN SCHOOL, RAS AL KHAIMAH

Acceptable Use Policy Agreement for School Parents

Background

.Computers and networks provide access to resources as well as the ability to communicate with otherusers worldwide. Such open access is a privilege and requires that individual users act responsibly.We envision a learning environment where technology is a part of us, not apart from us. The tremendousvalue of technology and the information technology network as an educational resource faroutweighs the potential risks. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staffto be more creative and productive in their work. All users should always have an entitlement to safeaccess to the internet and digital technologies.

Awareness

- Parents will understand the importance of use of technology safely by their ward
- Firewall and other effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices, and data.
- Parents are aware of and can protect themselves from potential risk in their use of online technologies.

User Actions

In addition to there being clearly illegal activity, the school believes the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows:

User Actions		Acc eptable	Accepta ble for nominat ed users	Una cce pta ble	Unac ceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicat e or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution ofindecent images of children.				X
	Grooming, incitement, arrangement or facilitation of sexual actsagainst children				X
	Possession of an extreme pornographic image (grossly offensive,disgusting or otherwise of an obscene character				X
	criminally racist material UAE– to stir up religious hatred (or hatred on thegrounds of sexual orientation) - contrary to the Public Order Act 1986				X
	pornography			X	
	promotion of any kind of discrimination			X	
	threatening behaviour, including promotion of physical violence or mentalharm			X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy			X	
Infringing copyright			X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)			X	
Creating or propagating computer viruses or other harmful files			X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			X	
Use of social media on behalf of the school, including posting texts *1		X		
Use of social media on behalf of the school, including video/images *2		X		
***1 – The set up of an account on social media sites/apps MUST be approved by the school's E-Safety co-ordinator and that security settings are set high, so that the content is not visible to the general public.**				
***2 – There is a compiled list which identifies children who are NOT PERMITTED to be included inany image/video reproduction. The nominated users are responsible for ensuring that they are aware of the list and the children do not appear on any online platforms/social media/website.**				

Professional and personal safety I understand that:

- I understand that the school digital technology systems are primarily intended for educational use
  - I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupilsfrom accessing inappropriate materials.
  - I understand that use of technology will be monitored in school.
  - When communicating I will use the technology provided by school (e.g. email and school social mediaaccounts) in an appropriate and respectful manner
  - Personal use of school technology is only acceptable with permission.

  For the safety of others:
  - I understand that my son/daughter has agreed in the pupil acceptable-use policy not to search for or shareany material that could be considered offensive, harmful or illegal. This might include bullying or extremist/hate/discriminatory content.
  - I will communicate with others in a respectable manner
  - I will share other's personal data only with their permission.
  - I understand that any images I publish will be with the owner's permission and follow the school's code of
    practice.
  - I understand the school has a clear policy on "The use of digital images and video" and I support this for
    the safety of the school I understand that
  - I understand that the school will necessarily use photographs of my child or including them in videomaterial to support learning activities.
  - I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, tothe appropriate person.
  - I will not deliberately bypass any system designed to keep school safe.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal

equipment to record theseimages unless I have permission to do so.

- I will inform the appropriate person in case of any damage to equipment or technologyI will not upload videos or images of any student, teacher or anything related to the School or tag anyone without prior consent from students, parents and from the school

I understand that the school takes any inappropriate behaviour seriously and will respond to observed orreported inappropriate or unsafe behaviour.

I have read and fully understand the contents of the school's e-safety policy.

Name ***Signature*** ***Date***

INDIAN SCHOOL, RAS AL KHAIMAH

Acceptable Use Policy Agreement for Schoolstaff/volunteers

Background

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.We envision a learning environment where technology is a part of us, not apart from us. The tremendous value of technology and the information technology networkas an educational resource far outweighs the potential risks. These technologies canstimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productivein their work. All users should always have an entitlement to safe access to the internet anddigital technologies.

Awareness

- Staff and volunteers will act professionally and use technology safely
- Firewall and other effective systems are in place for the online safety of all users and the security of devices, systems, images, personal devices, and data.
- Staff and volunteers are aware of and can protect themselves from potential risk in their use of online technologies.

The term "professional" is used to describe the role of any member of staff, volunteer or responsible adult.

User Actions

In addition to there being clearly illegal activity, the school believes the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain Internet usage as follows:

User Actions		Acceptable	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shallnot visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	**Child sexual abuse images –The making, production or distribution ofindecent images of children.**				X
	Grooming, incitement, arrangement or facilitation of sexual acts				X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character)				X
	criminally racist material in UAE – to stir up religious hatred (or hatred onthe grounds of sexual orientation) - contrary to the Public Order Act 1986				X

remarks, proposals or comments that containor relate to:	**Pornography**			X	
	Promotion of any kind of discrimination			X	
	Threatening behaviour, including promotion of physical violence or mentalharm			X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute			X	
Using school systems to run a private business				X	

Using systems, applications, websites or other mechanisms that bypass the filtering or othersafeguards employed by the school / academy			X	
Infringing copyright			X	
Revealing or publicising confidential or proprietary information (eg financial / personalinformation, databases, computer / network access codes and passwords)			X	
Creating or propagating computer viruses or other harmful files			X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)			X	
Use of social media on behalf of the school, including posting texts *1		X		
Use of social media on behalf of the school, including video/images *2		X		
***1 – The set up of an account on social media sites/apps MUST be approved by the school's E-Safety co-ordinator and that security settings are set high, so that the content is not visible to the general public.**				
***2 – There is a compiled list which identifies children who are NOT PERMITTED to be included inany image/video reproduction. The nominated users are responsible for ensuring that they are aware of the list and the children do not appear on any online platforms/social media/website.**				

Professional and personal safety I understand that:

- I understand that the school digital technology systems are primarily intended for educational use
- I will not engage in any on-line activity that may compromise my professionalresponsibilities.
- My use of technology will be monitored in school.
- When communicating professionally I will use the technology provided by school (e.g.email and school social media accounts).I am fully aware of the staff handbook regarding the use of my mobile device.
- Personal use of school technology is only acceptable with permission.
- For the safety of others: I will not access, copy, remove or otherwise alter any other user's files, without authorization.
- I will communicate with others in a professional manner, and I am aware that any communication made about a pupil to a member of staff via email is subject to data protection law.
- I will share other's personal data only with their permission.
- I understand that any images I publish will be with the owner's permission and follow the school's code of practice.
- I will only use school equipment to record any digital and video images with permission

For the safety of the school, I understand that

- I will not try to access anything illegal, harmful, or inappropriate.
- I will immediately report any illegal, inappropriate, or harmful material orincident, I become aware of, to the appropriate person.
- I will not deliberately bypass any system designed to keep school safe.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images unless I have permission to do so.
- I will inform the appropriate person in case of any damage to equipment or technology
- I will not install programs on school devices without permission
- I will not upload videos or images of any student, teacher or anything related to the School or tag anyone without prior consent from students, parents and from the school
- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises
- The official means of communication used among staff - Email, SMS, through the school portal - ERP and also through GSuite
- Established good review processes, to ensure that these technologies are developed the school and respond quickly to any potential online safetythreats through Firewall system

The sanctions that the school follow if the above policy / standard have been violated appropriate action will be taken.

I have read and fully understand the contents of the school's e-safety policy.

Name ***Signature*** ***Date***