ACCEPTABLE INTERNET USAGE POLICY

Aim

The aim of the Acceptable Internet usage policy is to ensure that all students and Staff are aware of the risks and hazards of Internet usage and use it sensibly and safely for the purpose of information sharing and improved learning. All students and Staff should be free of any fear of cyber bullying by anyone known or unknown. They should be able to recognise cyber bullying and be fully equipped to be able to deal with it effectively as well as be fully competent in surfing the Internet safely. All users competently use the web 2.0 tools to develop critical thinking and problem-solving skills enabling them to become effective global citizens.

Legal underpinning of the Policy

School is dedicated to complying with the UAE Federal Law no.2/2006 dated 3/1/2006: 'The Prevention of Information Technology Crimes' which provides clear guidelines regarding what is permissible and what is punishable in the usage of cyber space. School also assumes the responsibility of raising awareness against cybercrimes especially against children and training students, parents and Staff to be smart digital citizens.

Scope of the Policy

This policy includes:

- Acceptable usage of Internet by all students and staff within the School premises
- Anti-cyber bullying
- Improving awareness of intelligent usage of social media websites
- Smart usage of educational and information sharing websites
- Etiquettes of electronic communication

This policy has links to the following School policies:

- Behaviour Policy
- Child Protection Policy
- Health and Safety Policy
- Anti-Bullying Policy

Consultation

This policy has been developed in consultation with parents, staff and students, gathering their views through questionnaires, interviews, meetings and coffee mornings. The strong measures promoted by the UAE government also provided impetus in this regard. The growing number of cyber bullying incidents around the world and the increased usage of ICT in schools made it imperative to promote Internet safety.

Definitions

The School adopted the definitions of all terms related to Information Technology from the UAE Federal Law 2; The Prevention of Information Technology crimes, which gives the following definitions: -

Electronic Information	Means any information stored, processed, generated and transmitted by an information technology device in the form of text, images, sounds, numbers, letters, codes, signs or otherwise
Information Program	A set of information, instructions and orders executable by an information technology device and designed to accomplish a specific task
Electronic Information System	A group of software and devices for processing and managing electronic data, information, messages or otherwise
The Information Network / the Internet	A data communications system that interconnects information technology devices
Electronic Document	A record or document that is created, stored, generated, copied, sent, communicated or received by electronic means, on a tangible medium or any other electronic medium and is retrievable in perceivable form
Website	Data access point on the Internet
Information technology device	An electronic, magnetic, optical, electrochemical or other device used to process information and perform logical and arithmetic operations or storage functions, including any connected or directly related facility which enables the device to store information or communicate electronically

The School has used the definition of Cyber bullying by Cyber C3 (communication culture certification) which is a certification program run by the Khalifa University supported by the UAE government initiatives.

"Cyber bullying happens when a person is repeatedly harassed, mistreated, or made fun of via e-mails, websites, text messaging, cell phones, video, blogs or any other form of communication that occurs electronically".

This repeated and hostile behaviour that is designed to harm others through the use of internet and

computer communications can come from an individual or even a group.

Cyber bullying may include the following activities:

- Posting of slanderous messages on social networking sites,
- Spreading of rumors online,
- Excluding a person from an online group,
- Sending of unsolicited messages via text, instant messaging or email.

As this kind of bullying can take place anywhere, victims can no longer feel safe within their homes. This in turn causes great distress and negative impact on the victim's self-esteem and confidence."

Cyber C3 2012

Principles of Acceptable and Safe Internet Use

❖ The School places ownership on all Internet data that is produced, received or transmitted. This data can be revealed for appropriate requirement such as legal or investigative matters

❖ All electronic paraphernalia both hardware and software, expertise and services involved in the usage of Internet belong to the School and the School has the right to access and monitor all data and information interchange

❖ All emails sent through the School email system might be monitored to discourage use of offensive mails

❖ All sites and downloads may be monitored or blocked by school if the School considers them unsuitable or they are thought to be damaging to the School, staff or students.

❖ Unauthorised installation of software is not permissible at all.

❖ Usage of storage media which is not scanned prior to usage is strictly prohibited in order to limit spread of viruses and other malicious software.

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

➢ Using the web browsers for educational purposes of research and information gathering from various websites and databases

➢ Using the Internet for sharing documents and assignments promoting collaborative work

➢ Keeping the allocated personal username and password confidential and not sharing with anyone

- Not trying to access and change any other person's username, password, files or data
- Sharing emails only with people known to oneself and approved by parents or teachers
- Using Internet to do online tests or tasks approved or advised by the teachers
- Studying syllabus content online and performing tasks pertaining to it with teachers' authorisation
- Doing projects or presentations for the lessons
- Preparing circulars, invitations or information pamphlets for community service or other school activities with the teachers' approval
- Accessing examination sites for practice papers and answer schemes
- Responsibly accessing social websites for educational purposes only under teachers' guidance
- Always using appropriate language in all digital communications through emails, social websites, blogs or messages
- Taking good care of all digital devices in use.

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

- Being committed to responsible and effective usage of the Internet
- Using Internet only for School related purposes and not for personal matters
- Participating in all activities that help enhance and improve the professional aspect of any employee would be acceptable including online research and training
- Ensuring there is no unauthorised use of Internet by anyone in the School
- Using all available online teaching resources in the teaching and learning activities involving research and collaboration with other professionals in the educational field
- Enhancing the ICT skills and competencies of students to improve their learning
- Promoting the use of the Internet to support career counselling and investigating options for higher education most suited for individual students' interest.
- Supporting students' personal and social development through focused lessons with cross curricular links, cross country collaborative projects, e-learning and real life experiences
- Sharing good teaching practices involving advanced ICT skills through INSETS across School

Prohibited Uses of the School's Internet System for all users

- Using emails to threaten or harass other people
- Sending or posting disturbing images on the Internet
- Using Internet to commit any kind of piracy like music, film or software
- Sharing passwords or using and distributing passwords of others
- Violating the copyright law with respect to downloading or copying electronic files for personal usage
- Sharing School's confidential matters or information without authorisation
- Compromising the security of the electronic system of the School by introducing malicious software
- Using the Internet to promote personal business
- Visiting unauthorised websites
- Distributing any information which is incorrect, offensive or slanderous
- Using threatening and inappropriate language in communications
- Damaging the hardware or software installed in the school.
- Deliberately causing harm to someone's work or program
- Participating in cyber bullying
- Indulging in plagiarism which includes using someone else information or images of work without permission.
- Accessing pornographic sites or sites that promote hatred, discrimination or racism
- Disclosing personal information about oneself without authorisation
- Visiting social websites without authorisation
- Using someone else's information or images of work without permission
- Creating new accounts without the permission of School Principal
- Using school name, logo pictures on social media
- Sharing Edmodo username and passwords with each other
- Using someone else's information or images of work without permission.

Roles and responsibilities for student Internet Safety

1.School Leadership Team will:

- provide curriculum about appropriate etiquette for online behaviour, including awareness about interactions and communication with others on social networking websites and in chat rooms
- organise focused workshops on raising awareness of cyber bullying and appropriate responses in dealing with it
- ensure safety and security of students when using Internet and electronic communications
- provide students, staff and parents with guidelines and instructions for student safety while using the Internet

2.Students will:

- ensure they do not divulge any information about themselves or other persons on social media or through any other form of electronic communications over the Internet
- not disclose their home address or telephone numbers
- never upload any images of themselves or others without permission of parents or staff
- not plan or arrange appointments with anyone they have met on the Internet
- take proper measures if they receive any message that is inappropriate or makes them feel uncomfortable. They should immediately inform an adult they trust
- ensure they are not exposed to information or images that might harm them or cause them discomfort
- speak out against cyber bullying and immediately get in touch with the relevant Staff or parents
- avoid trying to access websites that have adult content and are restricted
- not damage computers, computer systems, software, or computer networks
- respect themselves and all other users through good network etiquette
- say no to plagiarism and give due credit to anyone whose work they are using for educational purposes
- help in raising awareness across School of acceptable and smart use of internet
- must not access any social media site, VPN whilst in school.
- personally, game consoles, owned portable media such as memory sticks and CD-ROMs may not be brought into school without specific permission beforehand.

3. Staff will:

- educate students about appropriate and safe Internet usage, including interaction and communication with other people on social networking websites and in chat rooms
- encourage awareness about cyber bullying and give clear guidelines as to the steps that are to be taken and people that can be approached
- monitor and ensure that there is no misuse of Internet
- raise awareness about the advantages and disadvantages of using social media.
- use the online web-based interactive communication technologies to enhance students' education and learning and to facilitate collaborative study habits in students
- improve peer collaboration and sharing of Internet resources through sustained usage of online web-based interactive communication
- empower students with 21st century learning tools to enable them to become independent learners
- share outstanding teaching practices through electronic communication
- develop cross country collaboration in students encouraging knowledge and skill based projects
- incorporate ICT in all areas of the curriculum to encourage the holistic approach of the students
- develop presentation skills using ICT for project work and competitions
- set clear expectations for students when engaging in online learning
- report to the IT department the URL (website address) and its content if they come across any unsuitable websites.
- should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

4.Parents will:

- Monitor and enforce their own family values to their children making them aware of the importance of using Internet safely
- Involve their children in regular discussions regarding the different challenges that are presented through the Internet
- Ensure that the children are aware of the acceptable Internet discipline and the consequences if the rules are broken
- Maintain clarity and consistency on what is permissible and what activities are unacceptable
- Assume complete responsibility for monitoring their children's use of Internet at home and outside School
- Have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions

- Inform and work with the School if any misuse is reported or found
- Seek help and support from the School in case of any incident that involves cyber bullying
- Be well informed about the work or projects given to the children to rule out any misuse. In case of any concerns they should check with the school immediately.
- Know the homework policy of the school well
- Set up parental controls, for example to only allow child to access age-appropriate content, or to monitor and block their usage.
- Discuss the importance of being respectful to others online, and the impact that their behaviour may have on people. Encourage them to consider the other person's perspective, and how hurtful remarks or actions could make someone feel.

Violations of this Policy

- The School reserves the right to terminate any user's access to School's Internet Systems - including access to School e-mail - at any time.
- If a student violates this policy their devices will be confiscated and appropriate disciplinary action will be taken consistent with the Discipline policy of the School and UAE by Law for Student Code of Conduct.
- If a student's access to the school Internet System is revoked, the student will not be penalized academically, and the teachers will ensure that the student continues to have a meaningful opportunity to participate in the educational program.
- Staff violations of this policy will be handled by suitable disciplinary measures.
- All users must promptly disclose to their teacher, parent, or line manager about any information they receive that is improper or makes them feel uneasy.

Promotion of the Policy

The policy will be promoted through circulars, coffee mornings for parents, and workshops for parents and students throughout the School. The message will be reinforced periodically by all teachers. Parents will be reminded through posters and informative circulars. Competitions revolving around raising awareness on this and related topics would definitely be beneficial. For Staff the policy would be promoted through INSETS, workshops and focus group discussions.

Monitoring and Evaluation

All Phases of the School will have a leader in charge leading the implementation of this policy. All teachers and Support staff would play the role in monitoring the usage in every class and within School. The IT department and web support would be supporting in evaluating the

information collected 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 investigation procedures, actions taken and subsequent next steps as well as the information collected from the 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.

This Policy was reviewed by the Senior Management Team. It will be next reviewed in August 2021.