E-Safety Policy

Reference number	APS – E-Safety Policy/ 2021/04/14
Version	Version 01
Review Schedule	Annual
Target audience	All Stakeholders of Amity Private School, Sharjah
Ratified by	Ms. Bandana Lazarus Principal
Ratified date	*April 2021*
Reviewed by	Mr. Nithin Thomas Head of Information Technology, Amity Corporate
Last Review date	April-2021

Contents

1. Online Safety Group

Title/ Designation	Name of the Member
Principal	Ms. Bandana Lazarus
Vice Principal	Ms. Alka Yadav
Online Safety Leader	Ms. Saritha Ajailal
Technical Support	Mr. Abdul Maajid
ICT Teacher	Ms. Sejal Vimal
Students	Ehsaan Faisal
	Amal Fathima
	Praneeth Jose
	Kriti Rai
	Ilhan Zaki
Teacher	Ms. Reena Choudhary
	Mr. Tamer Abdellatif Mohamed Abdelaziz

2. Scope of the Policy

The School is committed to promoting and safeguarding the welfare of students, staff, parents, caregivers, volunteers, visitors and the wider community. This policy applies to all members of the School community who have access to the School's Technology, whether on or off School premises or otherwise use Technology in a way that affects the welfare of students or any member of the School community or where the culture or reputation of the School is put at risk.

The policy and procedures are effectively communicated to the school community.
The school will deal with any incident referred to in this policy and associated behavior in conjunction with the other relevant safeguarding policies of the school.

3. Aims of the E-Safety Policy

- To protect and educate the whole school community from illegal, inappropriate and harmful content or contact in their use of technology.
- To inform the whole school community about their role in safeguarding and protecting APS community.
- To educate the students, staff, parents and visitors about their access to and use of technology.
- To establish effective and clear mechanisms to identify, intervene, escalate incidents, and monitor cases where appropriate.

- To put policies and procedures in place to help prevent incidents of cyber-bullying within the school community.

4. Roles and Responsibilities

4.1. The Governing Body

The Governing Body has an overall responsibility for:

- Safeguarding E-Safety arrangements within the School.
- The approval of the E-Safety Policy and for reviewing the effectiveness of the policy.
- To ensure that all those with leadership and management responsibilities at the School actively promote the well-being of students.
- To undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in the policy.

4.2. The Principal

The Principal has an overall executive responsibility and has a duty of care for ensuring the safety (including E-Safety) and welfare of the members of the School community.

4.3. The Senior Leadership (SLT) and E-Safety Team (EST)

Health & Safety Officer, E-Safety Leader, School Counselor, Wellbeing Coordinator, Technical Support.

- Managing and safeguarding incidents involving the use of Technology in accordance with the School's other Safeguarding policies.
- Responsible for ensuring that the E-Safety Leader and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues as relevant.
- To work along with the IT support manager to monitor use of Technology and practices across the School and engage in rigorous Self Evaluation to ensure the online safety and well-being of students and staff.
- To regularly monitor the IT Service Desk maintained by the IT Support Engineer/Manager.

4.4. IT Support Engineer/ Manager

The IT Support Engineer is responsible for ensuring:

- The school meets required E-Safety technical requirements as per regulatory authority (SPEA) OR other guidance that may apply.
- An effective operation of the School's filtering system so that students and staff are unable to access any material that poses a safeguarding risk, including extreme material, while using the School's network. It is secure and is not open to misuse or malicious attack.
- That an effective filtering policy is place and updated on a regular basis.

- That user may only access the networks and devices through a properly enforced and protected password and passwords are changed every three months.
- A regularly monitor of the use of the network/ internet/ Virtual Learning Environment (VLE)/ remote access/ email in order that any misuse/ attempted misuse can be reported to the Principal/ SLT/ EST/ E-Safety Leader.
- The Technology Incident Log is maintained and brings matters of safeguarding concern to the attention of the EST in accordance with the School's Child Protection & Safeguarding Policy and Procedures.
- To keep up-to-date E-Safety technical information in order to effectively carry out the e- safety role and to inform and update others as relevant.

4.5. All Staff

- To have an up-to-date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- To 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.
- To act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students.
- Staff has a responsibility to report any concerns about a student's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy. To report any suspected misuse or problem to the line manager for investigation/ action/ sanction.
- In lessons where internet use is pre-planned sites accessed by students to be verified as suitable for their use.
- All digital communications with students/ parents/ caregivers should be on a professional level and only carried out using official school systems.
- Staff have read, understood and signed the Staff Acceptable Use Policy/ Agreement (AUP)

4.6. Students

- Students above the age of 10 (Grade V and above) have read, understood and signed the Student Acceptable Use Policy/ Agreement (AUP) along with their parents at the time of admission.
- Are responsible for using the school digital technology systems at school, understand, and follow the E-Safety and Acceptable Use Policy.
- Students are expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on taking/ use of images and on cyber-bullying.
- Should understand the importance of adopting good E-Safety practices when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

4.7. Parents

- Parents have read, understood and signed the Parents Acceptable Use Policy (AUP)/ Agreement along with their child at the time of admission.
- Parents to promote safe practice when using Technology and to support the School in promoting good E-Safety practice and implementation of this policy and report any relevant concerns immediately.
- To ensure that their ward understands how to stay safe when using Technology is crucial.
- To ensure that their ward understand the need to use the internet/ personal devices/ mobile devices in an appropriate way.
- To follow guidelines on the appropriate use of Digital and video images taken at school events.

4.8. Visitors/ Community Users

- Visitors/ Community Users, who access school systems/ website as part of the wider school provision are expected to read, understand and sign a Visitors Acceptable Use Policy – Agreement before being provided with access to school systems.

5. Managing Acceptable Use

5.1. Education and Training

5.1.1. Students

- The safe use of Technology is integral to the School's Curriculum. Age appropriate guidance and access is given to students about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.
- Safety messages are reinforced through assemblies, Class Teachers Period (CTP) and tutorial/ pastoral activities.
- The School's Acceptable Use Policy for Students sets out the School rules about the use of Technology including internet, email, plagiarism, social media and mobile electronic devices, helping students to protect themselves and others when using Technology.
- Students are reminded of the importance of this policy on a regular basis.
- Students know how to protect themselves and peers from potential risks associated with use of technology.
- Students are encouraged to select and use technology for particular purpose.
- Students careful when they access online content and know how to validate accuracy of online information.
- They report cyberbullying and/ or incidents that make students feel uncomfortable or under threat.
- Students know how to treat each other's online identities with respect.

5.1.2. Staff

- All staff receive E-Safety training as part of their induction program, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- E-Safety training is provided to staff, which is regularly updated and reinforced.
- The school carries out a regular audit of the E-Safety training needs for all staff.
- The E-Safety Coordinator and staff receives regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations and regulatory bodies (SPEA).

5.1.3. Parents

- Parents are encouraged to read, understand and sign the Acceptable Use Policy for Students with their ward to ensure that it is understood fully.
- Parents to attend School based sessions on online safety.
- The school provide information and awareness to parents and caregivers through:
  - Letters, newsletters, School website.
  - Special events, workshops and campaigns e.g. Safer Internet Day.

Reference to the relevant websites/ publications and useful resources about the safe use of Technology is available via various websites including:

- Aqdar website- The site contains a wide range of information activities, Initiatives and links to other sites.
  - https://aqdar.ae/
- Cyber C3 Website - This site contains a wide range of information about safeguarding, child protection and how to protect yourself from online threats.
  - https://uaecyber.com
- Cyber C3 E-Learning
  - https://aqdar.cyberc3.ae/
- UAE Safer Internet Day Website
  - https://saferinternetday.ae/
- http://www.saferinternet.org.uk/
- https://www.internetmatters.org/
- http://www.thinkuknow.co.uk/
- https://parentinfo.org/
- http://educateagainsthate.com/

6. Managing Digital Content and Communication Technologies

6.1. Access to the School's Technology

- APS provides internet and intranet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email etc. to staff and students as per requirement.

- The school community uses school-owned technology equipment and personal devices utilizing the APS network, WAN network and private network.
- This Policy applies to privately owned devices accessing the APS/ WAN network – Internet connections while on school campus, or during events. As new technologies emerge, APS will seek to provide access to them. The policies outlined in this document cover all available technologies now and in future, not just those specifically listed or currently available.
- Students and staff use individual user names and passwords to access the School's internet and intranet sites and email system, which must not be disclosed to any other person. User names or passwords concern are reported and addressed by IT- Ticket Help Desk.
- Personal mobile electronic device may be connected to the School network with the consent of the IT support Engineer.
- All devices connected to the School's network should have current, up-to-date anti-virus software installed, and have the latest OS updates applied. The use of any device connected to the School's network may be logged and monitored by the IT Support Department.
- The School has a separate Wi-Fi connection available for use by visitors to the School. Use of this service will be logged and monitored by the IT Department. A password, which is changed on a regular basis, must be obtained to use the Wi-Fi.

6.2. Web Access

- APS provides its users the access to the Internet, including web sites, resources, content, and online tools.
- Access to the Internet is restricted as per regulations and school policies.
- Web browsing may be monitored and web activity records may be retained indefinitely.
- Users are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the Internet.
- Users should not use the unverified, incorrect, or inappropriate content.
- Users should only use trusted sources when conducting research via the Internet
- Whether a material is appropriate or inappropriate is determined on the basis of the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a request for website review through the APS Technology Service – Ticket Help Desk.

6.3. Communication - email/ social/ web/ collaboration

- APS provide users with the privilege of email accounts for the purpose of school-related communication.
- Users also get access to websites or tools that allow communication, collaboration, sharing, and messaging among users.
- Users should not attempt to open files or follow links from unknown or untrusted origins.
- Users should be careful not to share personal identity information online.

- Users should not post anything online that they would not want students, parents, teachers, or future colleges or employers to see. Once something is online, it is out there and can sometimes be shared and spread in ways that are not desirable.
- Email usage may be monitored and archived. Email accounts should be used with care.
- Users are expected to communicate with appropriate, safe, mindful, courteous conduct.
- Posts, chats, sharing, and messaging may be monitored.
- Netiquettes should be followed while online.

6.4. Downloads

- Users should not download or attempt to download or run.exe programs over the school network or onto school resources without the permission of the IT support Engineer.
- You may download other file types, such as images of videos. For the security of our network, download such files only from reputable sites and only for education purposes.

6.5. Plagiarism

- Users should not plagiarize content, including words or images from the Internet without citing the original creator.
- Users should not take credit for content they did not create themselves, or misrepresent themselves as an author or creator of something found online.

6.6. Personal Safety

- Communicating over the Internet brings anonymity and associated risks, therefore, always safeguard personal information such as phone number, birthday, address, ID numbers etc. of oneself and others.
- Young users should never agree to meet in real life someone they meet online without parental permission.
- Any message, comment, image, or anything else online that raises a concern for your personal safety should be brought to the attention of a member of the EST.

6.7. Security

- Users need to safeguard against the transmission of security threats over the school network.
- Users should not open or distribute infected files or programs and should not open files or programs of unknown or untrusted origin.
- If the computer or mobile device being used is suspected to be infected with a virus, please alert EST. This should be left to the IT technician to address.

6.8. Preventing Cyberbullying

- It is important to work in partnership with students and parents to educate them about Cyberbullying as part of our E-Safety curriculum. (Refer to APS Cyber Bullying Policy and Behavior Policy)

- Understand how to use these technologies safely and know about the risks and consequences of misusing them
- Report any incidence of Cyberbullying.

6.9. Use of Mobile Electronic Devices

- Special permission is required for a student to use their own mobile device and to connect to the Internet using the School's network. Permission to do so must be sought and given in advance.
- The School rules about the use of mobile electronic devices are set out in the Acceptable Use Policy Agreement for Students, Staff, Parents/Visitors.

7. Managing Digital Content

7.1. Social Media - Protecting Identity

- Use of social media for professional purposes is checked regularly as per Social Media Policy.
- School staff should ensure that No reference is made in social media to students, parents/ caregivers or school staff.
- School community members do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the School/ SPEA/ MOE.
- The school provides the following measures to ensure measures are in place to minimize risk of harm to students, staff and the school through limiting access to personal information.

8. Acceptable Use Agreement – Policy

The school has Acceptable Use Agreement Policy for the school community members

- Staff
- Students
- Parent/ Caregivers
- Visitor/ user

Monitoring and Review

S. No.	Version	Description of Change	Date
1.	1.0	Adoption of the Policy	April 2021

Principal | Ms. Bandana Lazarus : .....

Vice Principal | Ms. Alka Yadav : .....

Online Safety Leader | Ms. Saritha Ajailal : .....