مدرسة الإتقان الأمريكية

ALITQAN AMERICAN SCHOOL

E-SAFETY HANDBOOK

مدرسة الإتقان الأمريكية
ALITQAN AMERICAN SCHOOL

TABLE OF CONTENTS

POLICY REVIEW STATUS

Draft Review Date:	**18 February 2021**
Policy Review Date:	**20 January 2022**
Policy Approved Date:	**5 February 2022**

SUPPORT HOTLINES
Available from Sunday to Thursday during school days
8:00 AM to 2:00 PM

(06)5220010
0528875461

“For safety is not a gadget but a state of mind.”
-Eleanor Everet-

KEY OFFICIALS

Ms. Amani Araji
Environment, Health and Safety (EHS) Supervisor
COVID19 Task Force (CTC) Coordinator

sl01@alitqanamericanschool.com

Scope of Work: She ensures the school compliance for health and safety at school are met. She coordinates all the activities of the COVID10 Task Force and chairs the complaint center of the school.

Ms. Amal Hassan
Girls Supervisor
CTC – School Communication and Partnership

girlssupervisor@alitqanamericanschool.com

Scope of Work: She manages the administrative operations in the Girl's section and spearheads the effective system for school communication and partnership such as PTA.

Mr. Zaid Raddad
Academic Supervisor
CTF – Academic Affairs

as@alitqanamericanschool.com

Scope of Work: He manages the academic operations across the school in strong coordination with the educational supervisors.

Mr. Abourraya Ibrahim
Head of Inclusion and Boy's Social Worker
CTF – Student Affairs

boyssw02@alitqanamericanschool.com

Scope of Work: He manages the operations of the Inclusion program (SOD, Gifted and Talented Students) and matters related to student's wellbeing and classroom safety.

Ms. Maali Aryan, Junior Supervisor

juniores@alitqanamericanschool.com

Scope of Work: She manages the academic affairs in grade 1 and administrative operations in grades 1 to 3.

Mr. Nader Ibrahim, Boy's Supervisor

boyssupervisor@alitqanamericanschool.com

Scope of Work: He manages the administrative operations in the Boy's section which includes student's discipline.

FOREWORD

The E-safety policy at Al Itqan American school (AIAS) is developed as a response to the National Policy for Quality of Digital Life as approved by His Highness Sheikh Mohammed Bin Rashid Al Maktoum, the Vice President, Prime Minister of the UAE and Ruler of Dubai and His Highness Sheikh Dr. Sultan bin Muhammad Al Qasimi, a member of the Supreme Council of the United Arab Emirates, the Ruler of Sharjah, and President of the University of Sharjah. This handbook compiles policies and guidelines that promotes a positive identity and will create a safe digital community among all the stakeholders of AIAS.

In consideration that E-safety is constantly evolving & rapidly changing, the Senior Leadership Team of AIAS led by the current Principal Ms. Jessica Griffin in the late part of 2020 has initiated the formulation of the E-Safety team within the E-safety Framework for AQDAR E-Safe schools. Primarily, this has been conceived due to the following conditions:

1. There was a need to guarantee a safe environment among AIAS learners as their learning environment was shifted to online and remote brought by the impact of Pandemics on education.

2. Due to inevitable use of TECHNOLOGIES and the INTERNET, AIAS is prone to online predations that will negatively influence the confidence, authentic creativity and independence that are relevant to the development of digital skills for AIAS learners.

3. Academic staff particularly teachers must continuously be provided with standard guidelines toprotect AIAS learners and educate them further to thrive excellently in the educational delivery mode where the use of technology is required.

It must be noted that the policy indicated herein are all shaped by the current practice that are effective in the operation of the school and shall be reviewed and revised regularly when needed to ensure their effectiveness.

Special thanks to the team who put these policies together and studied their effectiveness in the AIAS Environment. Their hard work, patience and dedication in spite of the multitude of tasks are worth mentioning here for appreciation and acknowledgement:

Dr. Rommel Pelayo
Mr. Zeyad Al Sadi
Dr. Lavanya Ranganathan
Mr. Jebby Johns
Mr. Zaid Raddad
Ms. Amal Hassan
Ms. Amani Araji
Ms. Ola Bilal
Ms. Abeer Waleed
Ms. Akanksha Kar

And most importantly the inspiration that we get from our dear SLT led by the Principal, **Ms. Jessica Griffin** that collectively gathered all the ideas to form this handbook.

Part 1: Vision, Mission and Objectives Statements

Our Vision

We aspire to provide a digital learning environment where children are happy and love to learn.

Our Mission

We are committed to create a responsible and ethical safe learning environment for All.

Objectives

AIAS shall be committed to:

1. educate, support & create awareness to the individuals related to e-safety;
2. develop skills and knowledge to stay safe online;
3. facilitate the responsibility of using digital and internet technology;
4. reflect existing evidence of good practice in e-safety approaches;
5. provide information on how to handle online abuse if it occurs; and
6. facilitate access to age-appropriate support services including recovery services.

Part 2. Scope of the Policy

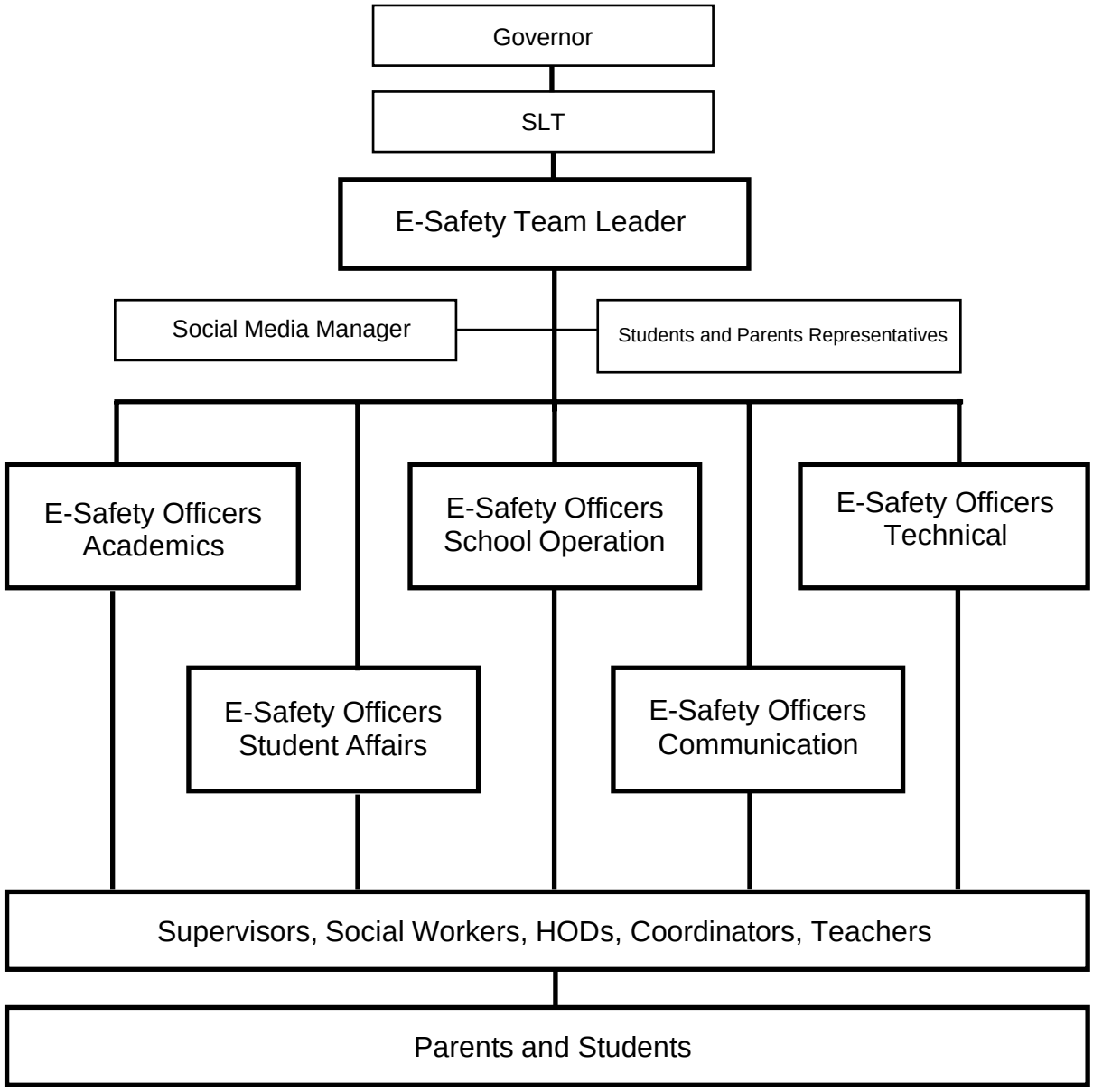
This policy is intended and applied to students, teachers and staff, visitors/guests who have access to the AIAS ICT system which are either internally or externally but related to the school. UAE National cyber laws and the National Policy for Quality of Digital Life empowers the school, to such an extent as is reasonable, to regulate the behavior of students when they are in and off the school site and empowers members of teachers/staff to impose disciplinary action for inappropriate behavior. This is relevant to incidents of cyber-bullyingor other e-safety incidents covered by this policy which may take place in and out of school but is linked to membership of the school. The school will deal with such incidentswithin this policy and associated behavior and use of digital content, well-being, child protection & safeguarding, anti-bullying policies and will, where known, inform parents/guardians of incidents of inappropriate e-safety behavior.

Part 3. E-Safety Committee

Section A. Hierarchy

The committee is primarily responsible for assuring a safe digital environment at AIAS. It is overseen by the school Governors and the SLT. The E-Safety Committee is spearheaded by the E-Safety team leader who coordinates all the E-Safety program of activities. Five E-safety officers work hand-in-hand with her along with the social media manager and representatives. Below is the organizational chart of the E- Safety Committee.

Figure: E-Safety Team Committee Chart



Section B. Job Responsibilities

Governor. The school governor is responsible for the approval of the E-Safety policy and for reviewing its effectiveness as they are laid down and implemented in school. They should receive e-Safety information and updates regularly.

Principal and The Senior Leadership Team. In consideration of the professional and ethical leadership responsibility of the Principal in the UAE context which states that the Principal should establish and maintain ethical behavior while using technology. The School Principal and the SLT are responsible to ensure that the systems for e-safety are in place and are embedded in the school culture:

1. The Principal and the SLT should promote the safety use of information and communication technology, provide equal access for all learners to information technology and its resources and demonstrates responsibility and provide technological cultural awareness.
2. The Principal and a member of the SLT should ensure that all the committee officers and team leader/coordinator receive adequate training to deliver the responsibility professionally.
3. The Principal and SLT should be fully aware of the E-Safety policy being implemented at school.
4. The Principal and the SLT should ensure that a system is in place for monitoring and support of those in school who carry out their e-safety monitoring role.
5. The Principal and the SLT attends regularly the monthly meeting, reviews and approves recommendations and proposals from the team.

E-Safety Team Leader. The team leader is primarily responsible for coordinating, monitoring and lead in the review of the activities and policies of the E-Safety at AIAS. The team leader is appointed by the SLT. Specifically, the E-safety team leader:

1. leads in the planning, implementation and evaluation of all the E-Safety program of activities at AIAS within the framework of the E-Safety Policy.
2. leads in the development, implementation and evaluation of the E-Safety strategic plan
3. assures that the school meets the requirements for local and international accreditation including but not limited to Aqdar accreditation for e-safe schools.
4. reviews the E-Safety policy regularly and propose changes required to the E-safety team and SLT.
5. evaluates the performance of the E-Safety team members regularly.
6. submits E-safety reports at the end of the term to the SLT indicating the progress of the conduct of the E-safety activities and the plan of action required to improve the delivery.

E-Safety Officers- Academics. The E-Safety Officer for Academics is primarily responsible for coordinating and leading the activities and policies of the Academic department of AIAS. SLT appointed the E-Safety Officer for Academics:

1. Leads in the planning, implementation, and evaluation of all the E-Safety Activities related to the Academic and Curriculum at AIAS within the framework of the E-Safety Policy.
2. Performs internal audit and assures that the Curriculum is up-to-date as per the E-Safety framework.
3. Reviews the curriculum regularly and propose changes required to the E-Safety team and to the SLT.
4. Conducts review meetings with the academic team and ensures that AIAS is achieving the targeted success on a regular basis.
5. Submits E-Safety Academic reports at the end of the term to the SLT indicating the progress of the conduct of the E-safety activities and the plan of action required to improve the delivery.

E-Safety Officers- Student Affairs. The E-Safety Officer for Student Affairs is primarily responsible for ensuring that AIAS is following the School Disciplinary Policy which aligns with the E-Safety Policy Framework. SLT appointed the E-Safety Officer for School Discipline:

1. Leads in the planning, implementation, and evaluation of all the E-Safety Activities related to the School Discipline at AIAS within the framework of the E-Safety Policy.
2. Performs an internal audit every 6 months and reviews the effectiveness of the SchoolDisciplinary Policy.
3. Reviews the School Disciplinary Policy regularly and propose changes required to the E-Safety team and to the SLT of AIAS.
4. Ensures that any issue related to the School Discipline is correctly reported and documented and escalated to the external agencies if required.
5. Always available for immediate response on any disciplinary issues happened inside the School premises or in Online sessions.
6. Leads the primary investigation team on the occasion of a possible cyberbullying or any issues related to E-Safety of AIAS.
7. Conducts team review meetings and ensures that AIAS is achieving the targeted success on bringing down the disciplinary cases.
8. Submits E-Safety School disciplinary reports at the end of the term to the SLT indicating the progress of the conduct of the E-safety activities and the plan of action required to improve the delivery.

E-Safety Officers- School Operations. The E-Safety Officer for School Operations is primarily responsible for ensuring that all staff of AIAS are aware about the E-Safety Policy Framework and they receive proper training on it. SLT appointed the E-Safety Officer for School Operations:

1. Leads in the planning, implementation, and evaluation of all the E-Safety Activities related to the School Operations at AIAS within the framework of the E-Safety Policy.
2. Performs an internal audit every 6 months and reviews the effectiveness of the E-Safety curriculum training and implementation of E-Safety policy in School.
3. Reviews the training schedule regularly and proposes changes required to the E-Safety team and to the SLT of AIAS to make it more effective and friendly.
4. Ensures the student awareness programs by creating E-Safety related posters and notices and are displayed in School bulletin boards, notice boards and classrooms.
5. Conducts team review meetings and ensures that AIAS is achieving the targeted success on training and implementation of E-Safety framework.
6. Submits E-Safety School Operations reports at the end of the term to the SLT indicating the progress of the conduct of the E-safety activities and the plan of action required to improve the delivery.

E-Safety Officers- Technical. The E-Safety Officer for Technical Aspects is primarily responsible for ensuring the total technical support and facility to all staff of AIAS. SLT appointed the E-Safety Officer for School Operations:

1. Leads in the planning, implementation, and evaluation of all the E-Safety Activities related to the School Technical Aspects at AIAS within the framework of the E-Safety Policy.
2. Performs an internal audit every 6 months and reviews the effectiveness of the of E- Safety policy in the proper use of all the technologies in the School.
3. Ensures that all gadgets are up to date and in good working condition.
4. Firewall must be regularly monitored and ensure that the filtering policy is effective.
5. Keeps record on all the network security accessories and maintains physical security to all of them.
6. Ensures that the School data is protected, and regular backup is taken.
7. Conducts team review meetings and ensures that AIAS is achieving the targeted success on the effective use of technology as per the E-Safety framework.
8. Submits E-Safety School Technical reports at the end of the term to the SLT indicating the progress of the E-safety policy and the plan of action required to improve the delivery.

E-Safety Officers- Communication. The E-Safety Officer for Communication is primarily responsible for ensuring the total communication support and facility to all staff of AIAS. SLT appointed the E-Safety Officer for Communication:

1. Leads in the planning, implementation, and evaluation of all the E-Safety Activities related to the School Communication at AIAS within the framework of the E-Safety Policy.
2. Ensures that the incidence logbook is accessible to all and reviews the incidence from the sheet daily and reports to the concerned staff all incidences for immediate action.
3. Performs internal audit every 6 months and reviews the effectiveness of the of E-Safety policy in the proper use of all communication channels in the School.
4. Ensures that all announcements and memos are made through the proper channel delivering a high standard of verbal and written communication.
5. Monitors the official social media accounts of the School and ensures that the content posted aligns with the E-Safety policy and the policy of UAE.
6. Always makes sure that the required consent form is signed before posting the content of any student or staff.
7. Ensures the regular update of social media account with the latest news and posters related to E-Safety.
8. Conducts webinars and trainings in social media which is related to the E-Safety.
9. Conducts team review meetings and ensures that AIAS is achieving the targeted success on the effective use of social media as per the E-Safety framework.
10. Submits E-Safety reports related to the social media communication at the end of the term to the SLT indicating the progress of the E-safety policy and the plan of action required to improve the delivery.

Supervisors, Social Workers, Section Coordinator, HODs, Event Coordinators and Teachers. They are responsible for reinforcing the e-safety policy in their respective areas of purview. This includes but not limited to:

1. read and understand the acceptable use of technology and ICT systems / agreement.
2. have an up-to-date knowledge of the current e-safety policy and practices
3. investigate and act on any incident where students, teachers and staff are at threat while using technology and ICT systems.
4. provide education to all stakeholders about the school's e-safety policy in varieties of ways.
5. carry out a communication system in an up-to-date and in a professional way.
6. ensure that the e-safety themes are embedded in the curriculum.
7. monitor the use of digital resources, mobile technologies, cameras, and the like in lessons and in school events and ensure that the related policy are reinforced.
8. make students understand the acceptable use of digital resources and technologies and provide continuous awareness sessions to them based on their needs.

Students

1. read and understand the acceptable use of technology and ICT systems in accordance to the Student Acceptable Use Policy.
2. should understand the regulations of e-safety at school and are aware of its importance.
3. have a good understanding of adopting the e-safety practices when using digital technologies and ICT systems and realize the coverage of the e-safety policy at school.
4. reports any form of abuse, misuse or access to inappropriate materials to their homeroom teacher or respective social worker or supervisor.

Parents

1. Support the school in promoting e-safety policy and practices and follow the appropriate guidelines in the use of digital and video images taken at school events; have access to parent portal and their children's personal devices in the school.
2. Report to the school any abuse, misuse or access to inappropriate materials for investigation.
3. Read and understand and sign the e-safety policy and practices in the content of acceptableuse.

Part 4. Statement of Policies

Section A. Reviews, Monitoring and Auditing

1. The overall monitoring and overseeing of the E-safety policy shall be made by the SLT in coordination with the appointed E-Safety Team leader. E-Safety activities should be approved and monitored by the E-Safety Team Leader in consultation and final approval of the SLT. Activities should be reviewed regularly.
2. The Governing body shall receive an annual report of the implementation of the E-Safety Policy generated by the implementing group made up of the team leader and officers.
3. E-Safety team should meet each term to review E-Safety activities and policies and engage the representatives in crucial decisions or even earlier whenever needed. The review includes but is not limited to the trainings and awareness campaign, E-Safety curricular implementation and the implementation of the E-Safety Policy in the classroom and at school in general.
4. Should there be a seriousE-Safety threat take place, the SLT particularly the Principal and the Vice Principal should be immediately informed.
5. The school shall monitor the impact of the policy through the following:
    a. Digital log sheets of the incidence
    b. Investigation Reports
    c. Lesson Observation Sheets of E-Safety Integration in the lesson
    d. Internal Audit report

Section B. E-Safety Education

B.1. Curriculum

Education is considered essential in promoting a culture of E-Safety at school. There should be a balance between the regulations with the education of students, teachers, parents, and staff to take on a more responsible approach to safety.

1. The school should have a curriculum guide for teachers to integrate e-safety in the lessons. This curriculum should contain the standards, performance expectations and big ideas that are relevant to promote safety education.
2. Curricular integration should revolve in the following safety theme namely (a) Online bullying; (b) managing online information; (c) privacy & security; (d) copyright & ownership; (e) online relationship; (f) self-image & integrity; (g) online reputation and (h) Health, well-being & lifestyle.
3. Each theme must be developed with digital citizenship activities that helps students build pathways that link a positive digital self-image with digital etiquette. The best practices for positive interaction on the digital medium and online safety to safeguard against threats should be covered.
4. E-safety awareness can be delivered in all grade levels through school events such as but not limited to Safer Internet Day, Tolerance Day, Kindness Day etc. Students and staff can be given recognition for their consistent over and beyond expectations of E-Safety practices at school.

B.2. Teaching and Learning

1. Curriculum delivery in the lesson should be meaningful and relevant which includes the following indicators for teaching: (a) Students are encouraged to demonstrate digital literacy skills in knowledge acquisitions and transference; (b) Students are provided with Cyberbullying awareness education and (c) Students follow health and safety protocols.
2. E-safety practices in remote teaching should be reinforced all the time. This includes (a) encouraging students to open their camera and b) ensure that only registered students are allowed to join the video conferencing.
3. Waiting rooms should always be activated particularly in Zoom conferences with caution.

Section C. Training

In consideration of the importance of having a safe online environment, all members of the community should receive adequate training and education required on E-safety policy and safe practices:

1. Teachers, staff and parents should be trained regularly on the E-safety standards. A needs assessment shall be administered and analyzed as a basis for the formulation of the E-Safety training plan during the academic year. This is spearheaded by the PD Coordinator appointed by the Principal and in consultation

with the E-Safety Team Leader. No PD plan should be administered without the approval of the SLT.

2. E-safety training of teachers and staff can be delivered synchronously and asynchronously. Synchronous training can be whole group, small group or individually based on needs within the context of supported experiment.
3. Asynchronous training should be in a training matrix form that contains important elements which is given to the staff to complete in an adequate and reasonable period of time. The matrix should include the (a) success criteria; (b) learning experience and (c) optional activities.
4. E-Safety team leaders and officers should attend not less than 10 hours of synchronous training related to e-safety every year. Certificates of attendance should be documented properly in a training portfolio which are reviewed termly by the team leader.
5. Teachers and administrators should complete not less than 5 hours of synchronous E-safety training per year which must be documented in a portfolio. They should complete at least one asynchronous module per year.
6. All new staff should receive training as part of the induction program to be arranged by the HR in coordination with the E-Safety committee ensuring that they understand fully the safety policy and the agreement for acceptable use.
7. E-Safety policy and its updates shall be discussed during the departmental meeting or general meeting whatever is applicable to keep staff in the loop. Alternatively, staff shall be receiving updates of policy via email.
8. E-Safety Awareness Campaigns for students and parents should be provided in an academic year based on needs.
9. All trainings and awareness campaigns must be assessed and evaluated to ensure an effective impact on the organization following the Kirkpatrick Taxonomy levels namely (a) Level 1: Reaction; (b) Level 2: Learnings; (c) Level 3: Behavior; and (d) Result/Impact. The result of evaluation should be reviewed to inform action planning.

Section D. Communications and Reporting Incident

Emails shall be used as an official form in communicating internally. CLASS DOJO can be used by parents to officially communicate with teachers. Complaints should be logged digitally using the E-Safety Complaint form.

By general rule, teachers may cancel online lessons anytime if the safety of the students are at risk and should communicate with the students and parents the next steps to resume the classes. The following steps should be adhered to:

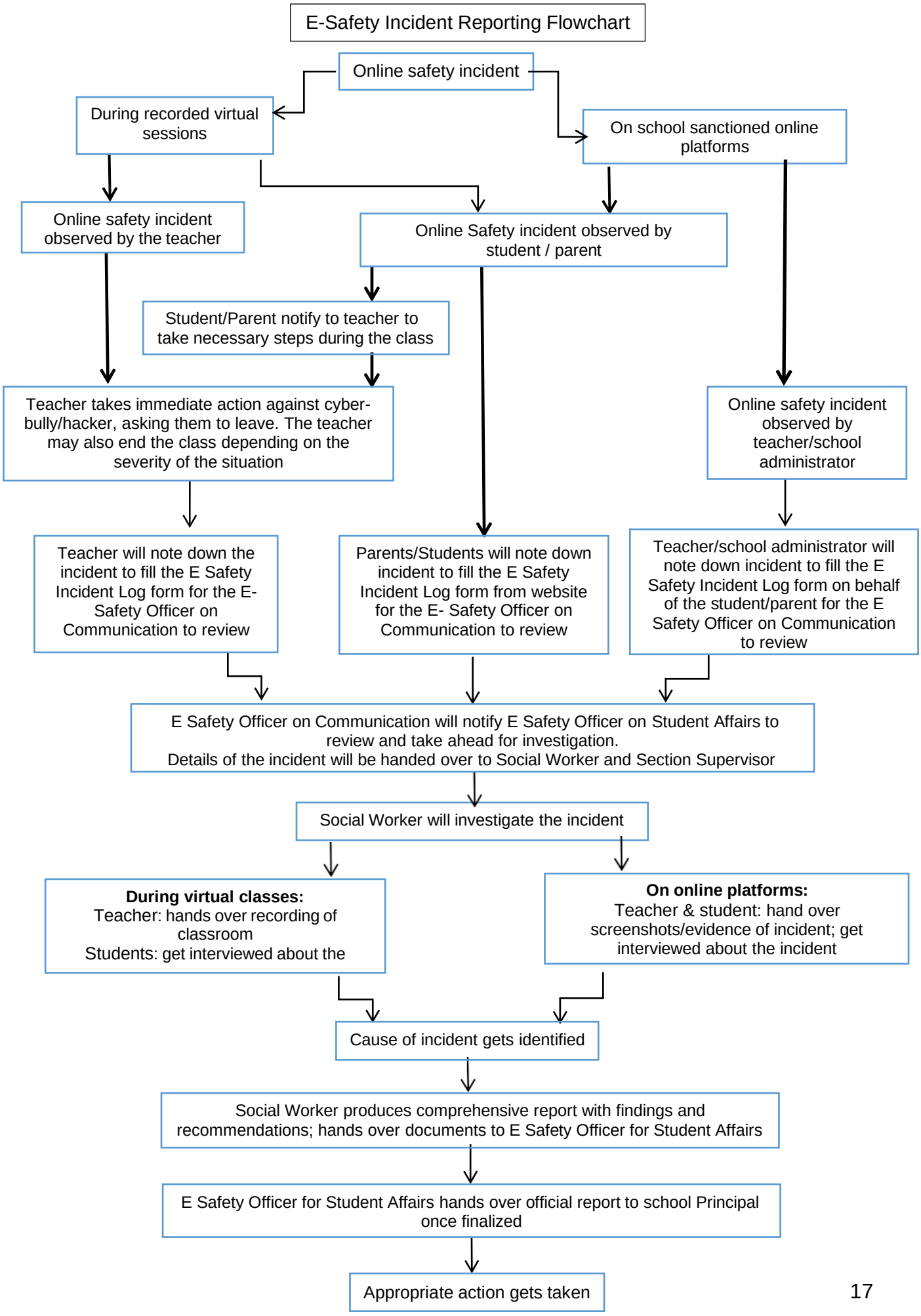
1. Students may report the incidents to their subject teacher or homeroom teacher whatever or whoever is applicable. They, in turn, log the incident to the E-Safety Incident Log Form from the school website which are reviewed by the E-Safety

officer on Communication. Daily incident should be coordinated to the E-Safety officer on Student Affairs for investigation.

2. Incidents shall be investigated by the Social Worker(s) along with the supervisor with the report submitted to the E-safety officer on Student Affairs for further review. The investigation should include (a) description of the complaints; (b) results and findings; (c) conclusions and (d) Recommendations. Reports must be approved by the Principal before final action is done.

3. Any teachers, administrators and staff who receive complaints should log them on the same e-safety incident form and communicate them to the supervisors for immediate follow-up.

The chart in the next page shows the flow chart when reporting and communicating the incident on e-safety.


E-Safety Incident Reporting Flowchart
Online safety incident
During recorded virtual sessions
On school sanctioned online platforms
Online safety incident observed by the teacher
Online Safety incident observed by student / parent
Student/Parent notify to teacher to take necessary steps during the class
Teacher takes immediate action against cyber-bully/hacker, asking them to leave. The teacher may also end the class depending on the severity of the situation
Online safety incident observed by teacher/school administrator
Teacher will note down the incident to fill the E Safety Incident Log form for the E-Safety Officer on Communication to review
Parents/Students will note down incident to fill the E Safety Incident Log form from website for the E- Safety Officer on Communication to review
Teacher/school administrator will note down incident to fill the E Safety Incident Log form on behalf of the student/parent for the E Safety Officer on Communication to review
E Safety Officer on Communication will notify E Safety Officer on Student Affairs to review and take ahead for investigation.
Details of the incident will be handed over to Social Worker and Section Supervisor
Social Worker will investigate the incident
During virtual classes:
Teacher: hands over recording of classroom
Students: get interviewed about the
On online platforms:
Teacher & student: hand over screenshots/evidence of incident; get interviewed about the incident
Cause of incident gets identified
Social Worker produces comprehensive report with findings and recommendations; hands over documents to E Safety Officer for Student Affairs
E Safety Officer for Student Affairs hands over official report to school Principal once finalized
Appropriate action gets taken

Section E. School Social Media

1. Social media is managed by the assigned person appointed by the Principal. Alternatively, the account details are also managed by the IT Officer.
2. Facebook, Class Dojo and Instagram are the school's official social media accounts. No other social media apps shall be permitted to be used by the school without the approval of the SLT and the CEO.
3. Request for any relevant posting requires approval of the Principal through the social media manager. Postings that are not intended for education or relevant to AIAS are not permitted.
4. Only pictures and videos of students with parent's consent are posted in the school social media account. Although selections are random, students must be appropriately dressed. Actions and words, if any, should be respectful and in an appropriate context. No pictures, videos or posts shall be uploaded in the school's social media account without the consent and approval of the Principal.
5. School has the rights to remove derogatory comments against any students, teachers and staff or about AIAS at any time and report the account to the social mediatechnical support. Social media manager may also block such account providedthat the recommendation be approved by the E-Safety team leader and the Principal.
6. In case the social media is hacked, the IT Officer should report it to the social media technical support for deactivation.

Section F. Disciplinary Policy

AIAS students are expected to exemplify an appropriate behavior as stipulated in the Student Code of Conduct. AIAS discipline is corrective rather than punitive. As such, AIAS shall be implementing both enhancement and reinforcement strategies as stipulated in the school's discipline handbook.

1. Social Workers, section coordinators and supervisors may give incentives to students who have exemplified over and beyond acceptable behavior when using the technologies and the internet such as:
    a. Points are awarded in the Class Dojo of the students under E-safety. Students who have reached a maximum point during a specific period shall be awarded with certificates every end of the term.
    b. Awardees should not be involved in any e-safety discipline issues during a specified period of time.
    c. Lists of awardees must have approval from the Principal before release.

2. Demerit points are also added in the Class Dojo for reinforcement and documentation.

3. All discipline issues related to e-safety threats including inappropriate comments should be properly investigated by the social worker and the section supervisors and the report should be reviewed by the E-Safety Officer on Student Affairs before

sending to the Principal for approval. The school shall reinforce the current UAE cyberlaw on these cases including federal penalties.

4. In the event of a major infraction of discipline, a discipline committee shall be called upon to make decisions. This includes the decision for involving police and the Child Protection whenever needed. The committee is comprised of the following members to be called a meeting in quorum:
    a. SLT
    b. Section Supervisor or Educational Supervisor
    c. Social Worker
    d. E-Safety Officer on Student Affairs
    e. E-Safety Team Leader
    f. Parent Representative
    g. Student Representative

Section G. Technological Gadgets, Software and Internet

G.1. Bring Your Own Device (BYOD).

All AIAS students shall use their own device in accessing learning resources and video conferencing during remote (online lessons) and in-class lessons (hybrid or face-to-face). To ensure safety in the use of their devices at school, the following points needs to be strictly considered:

a. Mobile gadgets that require the use of SIM cards are not permitted to students except teachers, administrators and staff.
b. Students and staff are responsible for safe-keeping of their own device. In case of lost, they should be reported immediately to their respective supervisor for further investigation. However, the school shall not be responsible for any damage and loss caused by their negligence.
c. Students' devices can be subject for inspection at any time during the day to ensure compliance of the rules of internet connectivity. The device can be surrendered to the supervisor and/or IT Officer for inspection purposes.
d. Students are not allowed to use the device for activities like playing games, watching movies or sending messages or any inappropriate material etc.
e. Use of social media is strictly prohibited inside the school premises. Strict action will be taken if any student is found to be using social media.
f. All educational websites are open inside the school network. Students can request to open any websites related to the studies.
g. Use of VPN is strictly prohibited inside school network. Management level action will be taken against those who breach this policy.

G.2. Acceptable use of Technologies and ICT systems

The school is responsible for ensuring that the school infrastructure / network is as safe and 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 staff name in the above sections will be effective in carrying out their e-safety responsibilities:

a. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
b. There will be regular reviews and audits of the safety and security of school academy technical systems
c. Servers, wireless systems, and cabling must be securely located and physical access restricted
d. All users will have clearly defined access rights to school technical systems and devices
e. The IT Officer is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
f. Internet access is filtered for all users
g. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the 'Acceptable Use Agreement'
h. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed
i. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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
j. An agreed policy is in place for the provision of temporary access of "guests" (for example trainee teachers, support teachers, visitors, SPEA) onto the school systems
k. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

G.3. Safekeeping and Maintenance of Technological Gadgets

To ascertain the safekeeping and maintaining of all the technological gadgets, both the movable and non-movable gadgets must be protected and the usage must be duly monitored.

a. All gadgets must be always placed perfectly in their assigned locations.
b. Gadgets must be physically checked daily for any potential damage by the user.
c. Incident report must be filled immediately after a damage is found.
d. Section coordinators are responsible for all the technological gadgets inside the classrooms of their designated areas.
e. School iPads must be given after entering the data in records and get the signature of the user who borrowed.
f. All iPads must be duly sanitized and kept inside the tray for charging by the person in charge.

g. Only permitted staff are allowed to take the iPads home and no Students are allowed to do so.
h. Device request form must be filled by the staff who require the gadget and must be returned on the date mentioned in the request form.
i. All software must be checked for regular updates and reported every 30 days.
j. License renewal must be checked and renewed on a regular basis.
k. 24 hours physical security must be provided inside the school premises for all the technological gadgets.

G.4. Depreciation:

Every device has an expiration date. It must be either upgraded or replaced based on the current requirements.

a. Network cables must be replaced after every 5 years based on the condition.
b. All hard disks must be replaced with SSDs after every 4 years or based on the degree of productivity of the device.
c. Every printer must undergo periodic service on every 180 days. The data waste must be cleared and scattered ink must be cleaned.
d. Internet capacity must be measured based on the number of users and degree of usage and must be upgraded if needed.
e. Wired accessories must be upgraded to wireless upon replacement.
f. Damaged or replaced gadgets must be clearly entered in the asset management of the ERP system.
g. Damaged or replaced gadgets must be kept in the storage and should not be disposed of in the regular rubbish bin. Check for shops who buy damaged gadgets.
h. While disposing the gadgets, always make sure that all data is cleared from the devices.

Section H. Acceptable Use Policy (AUP)

H.1. Acceptable Use Policy (AUP) (AIAS Employees)

Below are the acceptable use policies which should be observed when using the school's technology and ICT systems:

1. All Staff should not use technology while in school and its ICT systems for phishingor engaging in identity theft; storing / distributing pornography or adult related content; promoting violence activities or any form of cyberbullying, making any offensive or discriminatory online messages to persons based on race, ethnicity, national origin, gender, gender identity, sexual orientation, age, physical or mental illness or disability, marital status, economic status, immigration status, religion, personal appearance, or other visible characteristics; infringing the intellectual property; soliciting or distributing digital information with the intent to create violence, cause personal harm or injury, or

to harass, threaten or cyberstalk another individual; and other related e-safety threats under UAE cyber law.

2. Staff should not take pictures of students or staff or any school activities and post their personal information in their social media accounts for their personal gain.

3. Only maximum of two devices are permitted to be connected to the AIAS system for teachers and administrators. Nannies and support personnel are permitted to have only one device connected to the system for school use only.

4. Staff should use the AIAS authorized staff network for WIFI connection. Staff should not attempt to hack or bypass the school network filters. Any threat to security policies will be considered as violation of the AUP policy and will result in disciplinary actions.

5. Staff are fully responsible to secure and monitor their own school accounts to include emails, staff portal, Exact Path, Seesaw, Class Dojo, NWEA accounts, e- books and many more. Accessing accounts of other staff is strictly prohibited and shall be subjected to disciplinary actions. Staff should use only their school email account to access any authorized applications identified by the school.

6. Never use the official email for any personal use, as the official email will be handover to the new staff once a staff member leaves the school.

7. Support staff are not allowed to use school WIFI connection unless they have any school related trainings. Temporary WIFI connection will be provided for such training purposes.

8. Plagiarism / copyright is a violation as per the School Policy. Staff should cite all web sources in their PPTs or any academic teaching activity. This also includes all forms of media on the Internet, such as graphics, movies, music, and text etc.

9. Staff are not allowed to answer calls using mobile phones during their classes and social media account during working hours.

10. No staff is allowed to use any external storage device through USB port inside the school desktop PCs.

11. For official file sharing and data storage purpose, all staff must use their official OneDrive.

12. For very large file transfer, staff must approach IT Officer to have required device scanned and approved to use.

13. Any e-safety threat or incident noticed by the staff then they should immediately report & follow the incident reporting & communication policy system of e-safety.

14. Staff are not to impersonate any person living or dead, organization, business, or other entity etc.

15. Staff should not disclose school trade secrets, or confidential or proprietary information, including student record information that are in digital form or written form, or share videos, and photographs without authorization or without proper security measures that violates UAE law, school rules, policy, or guidelines.

16. Staff should not falsify, tamper with, or make unauthorized changes, additions or deletions to data located on the School Network or School systems.

17. Staff should not install, download, or use unauthorized software or third-party system games, programs, files, electronic media, and/or applications from the unauthorized websites that may cause a threat to the School Network.

18. Staff should strictly adhere to the provisions of the E-Safety handbook and must be fully aware of the current policies being implemented. He/She must be subjected to disciplinary actions whenever provisions are violated under judicious investigations.

H.2. Acceptable Use Policy (AUP) (Students / Parents)

1. Laptops, Ipads and tablets that can only be connected to WIFI are allowed to be brought and used in school. Devices with SIM like mobile phones are not allowed.

2. Only one device is permitted to be used in the AIAS network.

3. Students are responsible to keep their own device with himself or herself at all times apart from when they are locked in their own locked cupboard. The school is not responsible for the security of their device.

4. WIFI connections will be managed by the IT personnel, in case IT support is needed for configurations or WIFI connections. IT personnel shall always disinfect these gadgets when handled.

5. Devices must not be used to cheat in a test or assignment.

6. Students must not capture, share or post photos or videos of staff or students or about the school activities on any site.

7. Even if the student uses his/her personal device, it must be surrendered to the school key official personnel anytime for inspection of misuse or hacking which includes, but not limited to, phishing or engaging in identity theft, storing / distributing pornography or adult related content, promoting violence activities or any form of cyberbullying, infringing the intellectual property and more.

8. Any form of damage to the reputation of the school / staff / students through online in the form of discriminatory harassment (race, gender, religious, physically challenged, sexual – orientation, age based) or any personal or psychological harassment through online will not be tolerated and shall be penalized as per the school's discipline policy and UAE

cyberlaw. The discipline committee has the right to issue disciplinary penalties as they deemed necessary based on the level and type of offence made.

9. Students who are members of any social media group that promotes hatred, discrimination or engaged in the propagation of immoral conduct and such group is publicized either in school or in the community shall be penalized in accordance to the degree decided by the discipline committee.

10. No online or offline games in the device to be played or downloaded and Students are not allowed to use social media during the school hours primarily intended beyond educational purposes.

11. Students should only use the AIAS authorized student network for WIFI connection. Students should not attempt to bypass the school network filters. Any threat to security policies will be considered as violation of the AUP policy and will result in disciplinary actions.

12. Students should disinfect their device regularly during school hours and should not be allowed to be shared with their classmates to avoid cross contamination.

13. Devices must be fully charged before they are brought to school. The school may not guarantee the availability of the charging points during school hours considering the observance of the social distancing rule.

14. VPN applications are prohibited. UAE National law will be applicable in this case.

15. AIAS encourages responsible use of the gadgets. They should only be used for purposes of education. Social workers may issue warning letters in case of continuous and intentional misuse.

16. School is not responsible for any damage and loss of their gadgets caused by irresponsible use and/or negligence. Students are fully responsible to take care of their gadgets at all times.

17. Students and parents are responsible for the security of their school accounts such as, but not limited to, the school portal, Seesaw, Exact path, Class Dojo MS Team and school emails. They should protect and secure these accounts against threats at all times.

18. All the policies related to school including BYOD, technology, behavior & e-safety policy should be strictly adhered to.

H.3. USB Protocol

1. No staff is allowed to use any external storage device through USB port inside the school desktop PCs etc.
2. For official file sharing and data storage purposes, all staff must use their official OneDrive.
3. Only IT Officer or the person authorized by the IT Officer is only allowed to use USB inside the school desktop PCs.

4. IT Officer must scan the USB using a premium Antivirus software before opening it in any system.
5. For very large file transfer, staff must approach IT Officer to have required device scanned and approved to use.

Section I. Digital Content

1. Digital content used in the lessons must be within norms of the Islamic values and traditions of UAE. This includes videos and pictures that are associated in the content. Teachers and trainers must review the content before using and assure compliance to the UAE educational laws. Any materials that are associated with religion other than Islam are not permitted.
2. Videos for purposes of education can be downloaded from the sources with appropriate acknowledgement from the author. The website and the author must be fully indicated below the video or within the presentation slides to protect the academic license.
3. Videos and other digital content to be used for education should be grade appropriate. Content that promotes or encourages violence, phishing, cyberbullying, copying of academic materials and other related e-safety threats are not permitted to be used.
4. Teachers and trainers are accountable in the digital content use in the lesson or in the training respectively. They should evaluate the accuracy and safety before use.
5. Lesson recordings are kept in the One Drive account of the teachers and are available to students and parents for viewing. These should be systematically managed by the teachers under the supervision of the HODs.
6. The school website and parent portal are the platform to archive parent memos, timetable, grades, learning matrixes and other resources for students and parents.
7. Teacher made resources such as learning booklets and PPT are archived in the school One Drive account managed by the HODs. Nearpod lessons should be accessed in the Nearpod library under the school account.
8. Class Dojo Portfolio and MS Team shall be used as a platform to archive student work arranged systematically.
9. Survey results, minutes of the meetings, progress reports and other relevant documents must be systematically documented in the school's One Drive account. A back up copy should be ensured other than those in the school drive.
10. Appointed staff by the SLT shall manage and supervise this data and ensure compliance with the policy stated herein.

Section J. Filtering Policy

Data filtering is the most important area in E-Safety. Any data can be accessed from the internet. But in AIAS, we filter the data using Fortinet E308 Firewall. This will safeguard our users from any potential virus or malware attack:

1. Firewall policy inside the firewall device must be updated regularly (every 30 days).
2. Different layers of network must be created for staff, students, admin and guests.

3. All social media sites must be blocked for students and guests.
4. Gaming, child abuse, pornographic, violent websites and contents must be filtered by the firewall and it should align with the filtering policy of UAE.
5. VPN filtering must be activated and updated regularly to block any new VPN created in the play store / app store.
6. All user log must be generated in the firewall for any future reference.
7. Regular alert must be given to all users in the event of any potential hacking or breaching of network from an external source.
8. IT Officer is only allowed to edit or update the policy of firewall with the approval of the SLT.
9. Approval from the SLT is required for those staff who must be excluded from the filtering.

Section K. Data Protection

K.1. General Confidentiality Statements

a. Electronic data must be stored on secure computer systems and should be handled by the authorized person who has access to information (using both physical and electronic means).
b. While sharing the data, it must be via secure channels and should not share more than is necessary for the task.
c. The sensitive personal data collected should be taken extra care to ensure that the personal information and privacy rights are protected.
d. All staff must attend regular data protection training and are all aware of their role in keeping the data secure.
e. Every credit card payment must be securely done with the payment provider. Other payment methods must be handled in a similar manner.
f. All staff and parents must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.
g. Appropriate access privileges of the different data classes must be assigned to different users according to their needs.
h. Users under school domain can only get access to our E-Learning platforms.
i. Public data intended for all users must be published in the school website, for example, school announcements.
j. Backing up the data must be done on a daily manner.
k. Never share the data with third parties for marketing or sales purposes or for any commercial use without the express consent.
l. All necessary information must be shared via secure channels like parent portal.
m. Data of the students and staff who left the school shall be archived but their accounts including, but not limited to, emails, Exact Path accounts, Seesaw Accounts etc. shall be de-activated.

K.2. Password Policy

n. Always the password should be kept secure and should not be shared with anyone.
o. Reset the password regularly and should not keep the same password more than 90 days.
p. Passwords must not be saved in easily accessible location like desktop or home page.
q. Never use the same pattern of password repeatedly they must be changed.
r. Never use the same password in all accounts.
s. Passwords of students, staff and parents must not be shared without proper authentication.
t. Network passwords must be changed every 90 days and should be shared only with the authorized persons.
u. Before changing the device, all passwords must be taken backup and must be erased properly from the old device.

Section L. Safety Centers

L.1. General Statements

Safety Center is the highly classified location inside AIAS where we keep all the confidential and sensitive data related to our School. It includes the personal data of our staff, students, parents and guests since the beginning of the school. Because of this, we have a strong policy to cover the security of our Safety Centers.

a. Safety Centers must be regularly monitored by the IT Officer of the school.
b. Every software used must be regularly checked for any updates every 30 days.
c. There is a daily check of the safety centers that it is connected to the internet and internallyconnected to all the PCs.
d. Always ensure that the data backup is taken automatically during the assigned time. Also, make sure that the PCs are turned on during the backup time.

L.2. Inside the School

e. Safety center inside the school premise must be under the regular supervision of IT Officer.
f. Regular power supply must be provided to the devices without fail. Immediate reporting must be done in an event of power failure.
g. Make sure that the safety center is connected to all PCs and it must be installed if a new PC is added to the School network.
h. Only authorized users can be given access to copy data from safety center.

L.3. Outside the School

e. A backup copy of safety center must be kept in a trusted and secured location outside the school premises.
f. AIAS safety center backup is placed in the residence of School CEO must beregularly monitored by the IT Officer.
g. The device must be always connected to the internet and make sure that the backup is copied automatically without any fail.
h. The backup device must be operated only during the event of any failure to the primary device.

L.4. Safekeeping and Maintenance of Safety Centers

i. Safety centers are under 24 hours CCTV surveillance.
j. Physical security must be given to the safety center room to avoid theft or fire.
k. Fire prone materials are strictly prohibited inside the safety center room.
l. Fire extinguishers must be placed inside the safety center room.
m. Only authorized persons are allowed to enter inside the safety center.
n. Checks on the health of data storage disks upon every 180 days.
o. Safety center room must always maintain 22 degree celsius of temperature.
p. Any maintenance work in the safety center must not last for more than 8 hours continuously.

Section M. Policy Enforcement

M.1. Documentation

a. Teachers and staff should acknowledge the receipt of the E-Safety Policy handbook which signifies that they read and have understood it. The signed agreement forms are compiled and safely kept by the HR.
b. Teachers should document their attendance and participation to training on e-Safety through portfolio. This is being monitored and tracked by the E-safety teamleader through the school's PD coordinator.
c. Relevant and updated documents of the e-safety such as, but not limited to, audit reports, policy handbook, accreditation evidences, incident log book summary sheets etc. should be kept in a digital folder managed by the E-Safety team leader and officer on technical aspects. These documents must be accessible to the committee whenever needed.

M.2. Monitoring Scheme & risk assessment for risk mitigation

i. Physical monitoring of the gadgets

    I. The One-to-One ratio of physical supervision of children must be done while using the Internet & actively monitoring all screen activity during lessons.

II. 40% of the student's gadgets must be monitored per month and checked regularly by the section supervisors on a random basis.

III. While monitoring the gadgets inside the class, the following parameters must be checked by the Supervisors.

a) *Whether there is any SIM card in the device?*

b) *Whether pornography / inappropriate content in the device?*

c) *Whether any device has games downloaded?*

d) *Whether students play games through apps inside the class?*

e) *Whether anyone using social media in the class?*

f) *Whether VPN is found in the device?*

g) *Whether more than 1 device with a student?*

h) *Whether anyone uses technology to cheat in the learning check/test?*

i) *Whether any photo or video of AIAS students/staff found in the device or shared with others?*

IV. While monitoring the gadgets outside the class (including hallways and corridors), the following parameters must be checked by the Supervisors:

a) *Are they taking any photos or videos of students/teachers/school activities inside the school?*

b) *Are they sharing the devices?*

c) *Are they sharing any content with others?*

M.3. Monitoring Flowchart

Monitoring flowchart