



# **AL AMEER ENGLISH SCHOOL, AJMAN**

## **SCHOOL E-SAFETY POLICIES**

**2022 - 2023**



We track Your Child's Future  
**al ameer**  
English School



نصحت لمستقبل أولادكم  
**الأمير**  
مدرسة الإنجليزية

# ***E-SAFETY POLICY 2022-23***

# INDEX

CONTENT	PAGE No.
Aims, Objectives and Scope of E-safety Policy .....	3
Monitoring / Review of Documents .....	4
Roles and Responsibilities .....	5-8
Policy Statements .....	9-10
Technical – infrastructure / equipment, filtering and monitoring .....	11-12
Data Protection .....	13
Communications .....	14-16
Incident Reporting .....	17-20
Appendices .....	21-25

## **Aims of the E-safety Policy**

- Protecting and educating students and staff in their use of technology.
- Informing teachers and parents/guardians about their role in safeguarding and protecting students at school and at home.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.
- Having effective and clear measures to deal with and monitor cases of cyber-bullying.
- Dealing with all current and relevant issues within the school, linked with other relevant policies, such as the Child Protection / Safeguarding, Behavior, Acceptable Use and Anti-Bullying policies.

## **OBJECTIVES:**

### **The School ensures that:**

- Students will be made aware of acceptable and unacceptable Internet use.
- Students will be taught, where appropriate, to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- Students will be educated about the effective use of the Internet.
- Students will be taught how to evaluate Internet content by ICT teachers.
- Students will be taught how to report unpleasant Internet content to their class teacher, supervisor.
- The school Internet access is designed explicitly for student use and includes filtering appropriate to the needs of our students.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites they visit.
- The use of Internet-derived materials by students and staff complies with copyright law.
- All students and staff understand the importance of password security and the need to log out of accounts.

## Scope of the Policy

- This policy applies to all members of the school (including staff, students, volunteers, parents / carriers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.
- The Policy of school empowers Principal to such extent as is reasonable, to regulate the behavior of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behavior. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.
- The school will deal with such incidents within this policy and associated behavior and anti- bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behavior that take place out of school.

## **MONITORING / REVIEW OF DOCUMENTS – 2022-23**

### **SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW**

This E-safety policy was approved by the Governing Body on:	11 March 2020
Monitoring will take place at regular intervals:	Annually (and as and when circumstances demand)
The implementation of this E-safety policy will be monitored by the:	E- Safety Team, Administrators and Middle Managers
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals.	Biannually (and as and when circumstances demands)
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online-safety or incidents that have taken place:	Regularly (and as and when circumstances demand)
Should serious online-safety incidents take place, the following persons should be informed:	Principal, Vice Principal, Supervisor, E-safety Coordinator, IT Coordinator

The school will monitor the impact of the policy using: (delete / add as relevant)

- Logs of reported incidents
- Surveys of reported incidents:

- Students
- Parents /Carriers
- Staff

## ONLINE SAFETY GROUP 2022-2023

Mr. S.J.Jacob - Principal

### **Mr. Saifudheen P. Hamsa- Academic Coordinator- ONLINE SAFETY PROGRAMME HEAD**

Mr. Nowshad Shamshudeen- Vice Principal

Mrs. Latha Anil Kumar - Curriculum Head

Mrs. Ahlam - Arabic Secretary

Mrs.Geetha – Girls section Supervisor

Mrs.Sheenu - Secretary

Mrs. Selma - Secretary

Mrs.Fathima - IT Coordinator

Mr. Navaz - IT Coordinator

Mrs. Bincy / Mrs. Shibini - Social Worker

Mrs. Jotsana - IT Head

### **Mrs. Anjaly Sujith - ONLINE SAFETY LEADER**

Mrs.Sheena Mary – IT Teacher

Mrs.Zeenath – Teacher

Mrs.Shazia - Teacher

Parent 1 Mr.Nowshad

Parent 2 Mr.Dileep

Parent 3 Mrs.Dhanya

Parent 4 Mrs.Simi Earnest

Student 1 - Head Boy - Afnan

Student 2 - Head Girl – Sheza Zain

### **DIGITAL AMBASSADOR:**

Jaishnavy Dev Sajeew – Girls – 12D

Thomas Philip – Boys – 10C

### **ASST. DIGITAL AMBASSADOR**

Fareeha Halima Abdul Kareem – Girls – 10D

Afsal Navas – Boys -12C

## **Roles and Responsibilities:**

E-safety -Roles and responsibilities of individuals and groups within the school:

### **Governors:**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Leader
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / Committee /meeting

### **Principal and Senior Leaders:**

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Principal and Senior Leaders are responsible for ensuring that the E- Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

### **E-Safety Coordinator:**

- Leads the e-safety committee
- Takes day today responsibility for e- safety issues and has a leading role in establishing and reviewing the school e- safety policies /documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff

- Liaises with the inspectors / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

### **IT Coordinator / Technical staff:**

The Co-coordinator for ICT / Computing is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and E- Safety Policy.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with e-safety technical information in order to effectively carry out their e- safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-safety Governor /Principal/Senior Leader/E-Safety Coordinator

### **Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Head of Year for investigation / action /sanction
- All digital communications with students / parents / careers

should be on a professional level and only carried out using official school systems

- E-safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copy right regulations
- They 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
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for the use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Child Protection / Safeguarding Lead**

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults /strangers
- Potential or actual incidents of grooming
- Cyber-bullying

### **Students:**

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Should read, understand and adhere to the Acceptable Use Policy and other policies.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice 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

- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and must be fully aware of the incident-reporting mechanisms that exists within school.
- Should be transparent in discussing e-safety issues with family or teachers.

### **Digital Ambassadors:**

Al Ameer English is one of the popular school in Ajman. The school is focused on ensuring the 100% of Cyber safe school.

As a Digital Ambassador, you will support the students to give an awareness about cyber issues. You will be responsible creating good Coordination with the students and report the cyber issues up-to-date with the Online Safety Leader.

#### **Key responsibilities and objectives of the role may include:**

- 1) To give awareness about cyber safety & Its Rules from KG to Grade 12
- 2) Record & Report the list of students who face any cyber issues with their – “Name, GR. NO., Class and Issue faced ”.
- 3) Discussing and solving the issues with ICT team through SLT.
- 4) Make sure to provide all kind of ICT support to the students at any time.
- 5) Ensuring all the students are following cyber safety Policy, Rules and Precautions.

### **Parents / Caregivers:**

Parents / Carriers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and caregivers will be encouraged to support the school in promoting good e- safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website /blog
- Their children's personal devices in the school (where this is allowed)

## **ROLES & RESPONSIBILITIES OF PARENTS FOR POST-COVID 19 CARE**

### **(Stress Management of Students)**

Children react to stress in many ways, and their reactions may vary depending on various factors, including age. Here are some signs:

- Children may experience ups and downs in their behaviors and their emotions may change. They may be unusually active, aggressive, quiet or sad.
- Children may express fear, become overwhelmed, and display anxiety. They may cry or become more clingy than usual. They may have disrupted sleep patterns.
- Children may become unwilling to participate in chores or schoolwork. They may also not get along so well with siblings and other family members.

- 1. Maintain communication with the teachers*
- 2. Share your personal school experiences*
- 3. Monitor their academic progress*
- 4. Appreciate positive outcomes*
- 5. Listen to their needs and desires and support where necessary*
- 6. Normalize failure*
- 7. Be calm and proactive*
- 8. Stick to a routine*
- 9. Let your child feel their emotions*
- 10. Check in with them about what they're hearing*
- 11. Keep them safe with open communication*
- 12. Use technology to protect them*
- 13. Spend time with them online*
- 14. Encourage healthy online habits*

*Remember that it is understandable for children to react to stressful situations. It is important that you recognize their stress and console them as is age appropriate.*

### **Community Users**

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

### **Policy Statements Education – students**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the e-

safety provision of the school. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned program of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials/content they access on- line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre- planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

**It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.**

### **Education – Parents / Caregivers**

Many parents and carriers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviors. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be

unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and caregivers through:

- Curriculum activities
- Letters, newsletters, website
- Parents / Caregivers meetings /sessions
- High profile events / campaigns e.g. E-safety Awareness Campaign/Anti-Bullying Campaign
- Reference to the relevant web sites /publications



## **Education – The Wider Community**

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience.

This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents
- The school / academy website will provide e-safety information for the wider community
- Supporting community groups (e.g. Early Years Settings, Child minders, youth / sports / voluntary groups) to enhance their e-safety provision

## **Education & Training – Staff / Volunteers**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A program of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff should receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organizations
- This E Safety policy and its updates will be presented to and discussed by staff in staff/team meetings
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

## **Training – Governors**

Governors should take part in e- safety training/awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the National Governors / or other relevant organization
- Participation in school training / information sessions for staff

## **Technical – infrastructure / equipment, filtering and monitoring**

The school will be 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 people named in the above sections will be effective in carrying out their e- safety responsibilities:

- School technical systems will be managed in ways that ensure that the school/academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices
- The Principal/the designated Officer is responsible for ensuring that software license logs are accurate and upto date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users
- School/academy 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
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident/ security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, 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 work stations are protected by up to date virus software

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Bring Your Own Device (BYOD)**

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy.

According to Al Ameer's Policy, BYOD devices will be denied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied.

### **Use of Digital and Video Images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parent's / care givers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide a venue for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or

embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognize the risks attached to publishing their own images on the internet eg on social networking sites
- In accordance with guidance from the Information Commissioner's Office, parents / caregivers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made

publicly available on social networking sites, nor should parents / careers comment on any activities involving other students / pupils in the digital / video images

- Staff and volunteers are allowed to take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or careers will be obtained before photographs of students are published on the school website
- Students' work can only be published with the permission of the pupil and parents or guardians.

### **Data Protection (followed as guidelines)**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

### **The school ensures that:**

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act(DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office

### **Staff ensures that they:**

- At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices
- Are not accepting friend requests from their pupils on their personal social media accounts.
- Are not following pupils’ personal social media accounts.
- Are not contacting pupils using their personal email address.

## Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person– in accordance with the school/academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents / caregivers' (email) must be professionally tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Whole class / group email addresses may be used at KS1, while student pupils at KS2 will be provided with individual school email addresses for educational use
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk School staff should ensure that:

- No reference should be made in social media to pupils, parents / caregivers or school staff
- They 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
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

## COMMUNICATION TECHNOLOGIES

Communication Technologies	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	Yes						Yes	
Use of mobile phones in lessons		Yes						No
Use of mobile phones in social time	Yes							No
Taking photos on mobile phones or other camera devices	Yes						Yes	
Use of school email for personal emails				No				No
Use of chat rooms / facilities							Yes	
Use of social networking sites				No				No

### **Social networking and personal publishing:**

- The school has a duty of care to provide a safe learning environment for all its students and staff and will ensure the following:
- Blocking student access to social media sites within school boundaries
- Educating students about why they must not reveal their personal details or those of others, or arrange to meet anyone from an online site
- Educating both students and staff as to why they should not engage in online discussion revealing personal matters relating to any members of the school community
- Educating both students and staff about ensuring all technological equipment is always password/PIN protected
- Informing staff not to accept invitations from students or parents/guardians on social media
- Informing staff about regularly checking their security settings on personal social media profiles to minimize risk of access of personal information

## UNACCEPTABLE USAGE POLICY

		Acceptable	Acceptable at certain times	Acceptable for certain users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images					<input type="checkbox"/>
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					<input type="checkbox"/>
	pornography				<input type="checkbox"/>	
	Promotion of any kind of discrimination				<input type="checkbox"/>	
	Promotion of racial or religious hatred				<input type="checkbox"/>	
	Threatening behavior, including promotion of physical violence or mental harm				<input type="checkbox"/>	
	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				<input type="checkbox"/>	
Using school systems to run a private business					<input type="checkbox"/>	

Use systems, applications, websites or other mechanisms that bypass the filtering.				<input type="checkbox"/>	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				<input type="checkbox"/>	
Revealing or publicizing confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				<input type="checkbox"/>	
Creating or propagating computer viruses or other harmful files				<input type="checkbox"/>	
On-line gaming (non-educational)				<input type="checkbox"/>	
File sharing				<input type="checkbox"/>	
Use of social networking sites		<input type="checkbox"/>			
Use of video broadcasting e.g. YouTube		<input type="checkbox"/>			

## INCIDENT REPORTING

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### **In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff/ volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by local organization
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - Incidents of ‘grooming’ behavior
  - The sending of obscene materials to a child
  - Adult material which potentially breaches the Obscene Publications Act
  - Criminally racist material
  - Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

---

## **Responding to Incidents of Misuse**

This guidance is intended for use when the staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

### **School Actions:**

It is more likely that the school / academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportional manner, and that members of the school community are aware that incidents have been dealt with.

## Actions (Students)

Incidents	Refer to class teacher	Refer to Co- coordinator s	Refer to Principal / Vice Principal	Refer to technical support staff for action re	Inform parents	Verbal Warning	Written Warning	Further sanction eg detention / exclusion	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Unauthorized use of non-educational sites during lessons	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>		
Unauthorized use of mobile phone / digital camera / other handheld device	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>				
Unauthorized use of social networking / instant messaging / personal email	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>		
Unauthorized downloading or uploading of files	<input type="checkbox"/>				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Allowing others to access school network by sharing	<input type="checkbox"/>				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

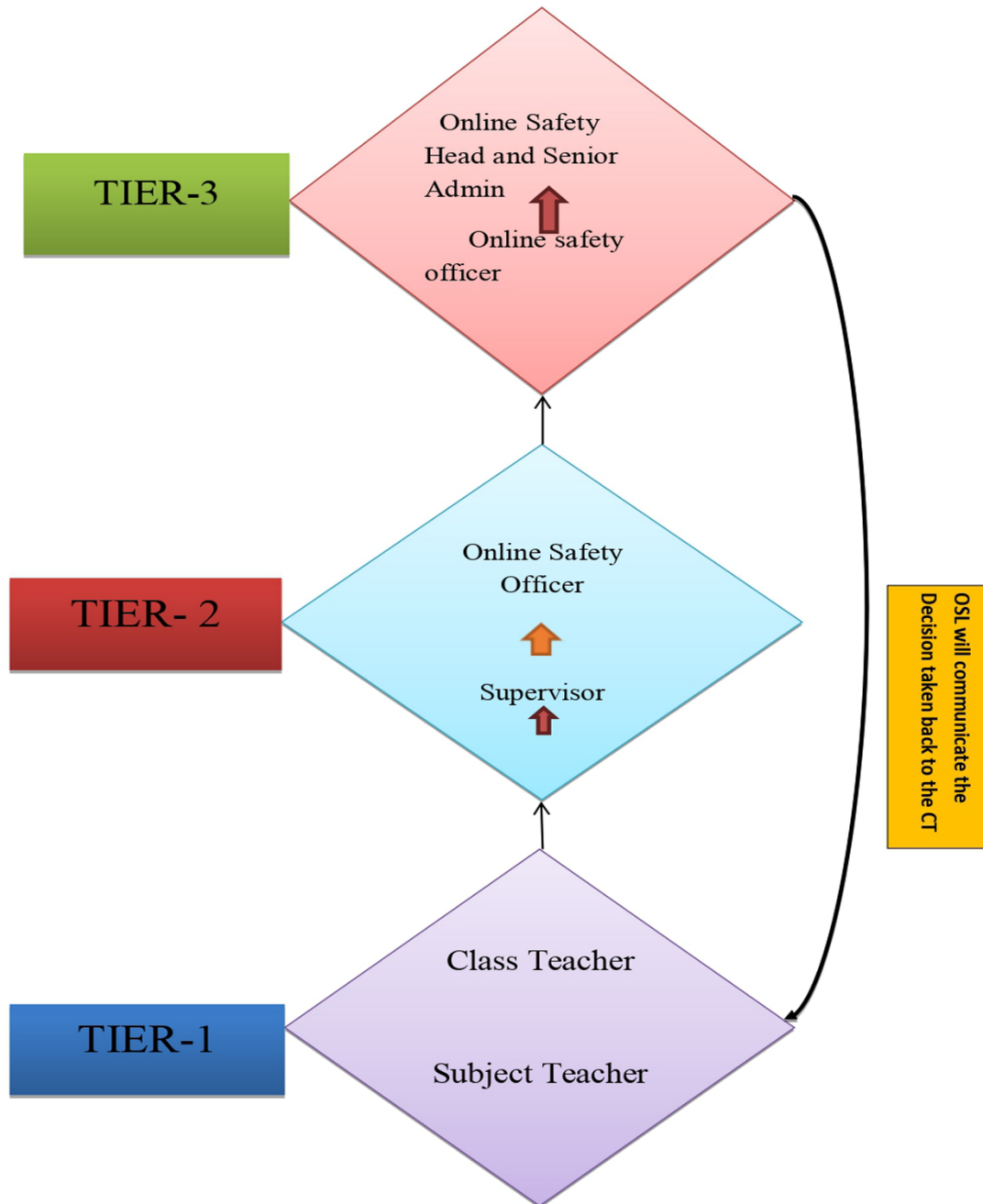
username and passwords									
Attempting to access or accessing the school network, using another student's account	<input type="checkbox"/>					<input type="checkbox"/>	<input type="checkbox"/>		
Attempting to access or accessing the school network, using the account of a member of staff	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>				

## Actions (Staff)

Incidents	Refer to Principal / Vice principal	Refer to Director s	Refer to technical support staff for action re	Warning	Suspension	Disciplinary action	Refer to Police
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	<input type="checkbox"/>	<input type="checkbox"/>					<input type="checkbox"/>
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	
Unauthorized downloading or uploading of files	<input type="checkbox"/>			<input type="checkbox"/>			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account				<input type="checkbox"/>			
Careless use of personal data eg holding or transferring data in an insecure manner	<input type="checkbox"/>			<input type="checkbox"/>			
Deliberate actions to breach data protection or network security rules	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>	<input type="checkbox"/>
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Actions which could compromise the staff member's professional standing	<input type="checkbox"/>			<input type="checkbox"/>		<input type="checkbox"/>	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>	

## COMMUNICATION PLAN FOR INCIDENT REPORTING



### Appendices:

- 1) Student & Parent Consent Form
- 2) Teachers & Staff Consent Form
- 3) Media Consent Form

## Students Online Acceptable Use Agreement

**AL AMEER regularly reviews and updates all Acceptable Use documents to ensure that they are consistent with the school Online Safety and Safeguarding Policies.**

These rules will help to keep everyone safe and to be fair to others. School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

1. I will be a responsible user and stay safe when using the internet and other digital technology at school.
2. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
3. I will only use the school's internet and any device I may be using in school for appropriate school activities and learning, unless I have express permission to carry out recreational activities, e.g. in a lunchtime club or afterschool.
4. I understand that all internet and device use in school may be subject to filtering and monitoring; I understand that all school-owned devices used outside of school may also be subject to filtering and monitoring, and should be used as if I am in school.
5. I will keep my logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it.
6. I will not bring files into school or download files that can harm the school network or be used to bypass school security.
7. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
8. I will use the internet, games and apps responsibly; I will not use any that are inappropriate for the school, my age or learning activities, including sites which encourage hate or discriminating against others.
9. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
10. I understand that cyber bullying is unacceptable, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside.
11. I will not browse, download, upload, post or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
12. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions and I should respect this.
13. I will only e-mail or contact people as part of learning activities.
14. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the school. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
15. When using the internet, I will not download copyright-protected material (text, music, video etc.)
16. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
17. Live streaming can be fun but I always check my privacy settings and if I rarely (or preferably never) do anything that everyone on the internet can see. If I live stream, I tell a trusted adult about it.
18. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.

19. I will only use my personal devices (mobile phones, USB devices etc) in school if I have been given permission to do so.
20. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
21. I understand that many apps have relocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn relocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
22. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
23. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, extremist/hateful content, I will not respond to it but I will save it and talk to a trusted adult.
24. I know that I can always say no online and end a chat or block a friend; if I do, it's best to talk to someone about it as well.
25. I know who my trusted adults are at school, home and elsewhere, but if I feel I can't talk to them, I know I can call Childline or click CEOP.

### **Parents' Role at home:**

- a. Keep the computer in a central place, where everyone can see what's on the screen. Stay involved (without stepping on their toes constantly) on what they are doing online—especially if it's got to do with searching and looking for new information etc.
- b. Tell them the “No-Can-Go” sites and “No-Can-Play” games rules ahead of time. Check out which sites they want to access, or which games they want to play and tell them if they are acceptable or no-go zones, until they reach a certain specified age.
- c. Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they can have a week.
- d. Explain online habits. Explain strangers often play pretend games and they are not really who they claim to be. Explain how sometimes a nine year girl from the US is really a 50 year old man from Bangkok. They need to be clearly told that no matter how interesting or “just like me” the stranger sounds like, they are not to respond.
- e. Switch Safe Search on as a setting. It's great that most inappropriate content does get filtered by Etisalat or du here in Dubai, but there are many slip ups and search results may often have content that's not age appropriate.
- f. Remind them that they should not engage in any form of cyberbullying – even in jest. They should not do anything online that they would be ashamed of doing in real life.
- g. Beyond online, watch what content you have on your computer. Often we receive email that is not age appropriate for our children, but we leave that in our mailboxes or desktops. Set the example, cleanup.
- h. If your children have started to do their homework online, or are gathering information, researching facts etc., explain to them clearly how they should not “copy and paste” (plagiarize) content for their homework, unless they mention sources etc. Their teachers should help them understand this, but you should make it clear that this is not on.

- i. Be involved. Be courteous. Be alert. Show on-going interest in what they are playing, reading, doing online. And always remind them that there is life (and a wonderful one) outside that screen.

### User compliance

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

*Name of the Student:* .....

*Name of the Parent:* .....

*Signature:* .....

*Signature:* .....

*Date :* \_\_\_\_\_

## Staff Online Acceptable Use Agreement

- I understand that the school will monitor my use of the computing systems and other digital communications on the school equipment.
- Sharing of confidential materials, such as, passwords, PINs, or other authentic information is strictly prohibited. Everyone is responsible for his/her account(s), including the safeguarding of access to the account(s).
- The use of WISE resources to, access, further or otherwise participate in activity which is inconsistent with the mission of the school is prohibited. This includes, but is not limited to the following: illegal activity, sexually explicit material, hate speech, violent behaviour & bullying, spam, hacking, etc.
- In addition to standard electronic resources, members of the school community are expected to make appropriate use of the school Telephone/mail system. Examples of inappropriate actions:
  - a. Unauthorized use of another individual's identification and password.
  - b. Use of the school telephone/mail system to send abusive, harassing, or obscene messages.
- Understand that the school computing systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- Will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. Will not take or distribute images or videos of anyone without their permission.
- Will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online. Will report any kind of security risks or violations in any form to IT administrator.
- Understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programs, apps or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials.
- Members of the staff are responsible for their computer, including its hardware, software, and any network traffic transmitted by it. Please contact IT Support group if you have any questions about whether certain software/hardware might conflict with this acceptable use policy.
- Will not try to open any attachments to emails, unless I know and trust the person/ organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programs/apps.
- The school reserves the right to examine, use, and disclose any data found on The school's information networks in order to further the health, safety, discipline or security of any student or other person, or to protect property. They may also use this information in disciplinary action and will furnish evidence of crime to law enforcement.

### User compliance

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Name of the Employee: .....

Employee's Signature: .....

Date: .....

## **Media Consent Form**

Dear Parent / Guardian

During the school year, we take photographs of school activities involving students to share the school's positive vibe and updates. By which incidentally, some photographs may capture your child's participation, directly or indirectly. These photos may be published through our website, social media pages, news bulletins, billboards, and ads etc. So we request you to carefully read the points below.

I understand that:

- My child's photograph may be used within the school for display purposes.
- My child's image may be used in Learning Journeys or Records of Achievement belonging to other children.
- My child's image may be used on the school website, school newsletter, school social media accounts e.g. Facebook, Instagram etc.
- My child's photograph may be used in local and/or national media.
- My child may be filmed by the school during school events.

### **Video Filming:**

During school events we accept that many parents may wish to film their child. However, all parents must agree to the following terms and conditions

- All filming is for personal use only and must not be shared with external agencies.
- No video, film or still photography from school events may be posted to any form of social media.

### **Terms and Conditions:**

- This form is valid for the period your child attends this school. Images of your child will not be used after this time.
- Please write to the Principal if you wish to withdraw consent at anytime.
- The images we take will be of activities that show the school and children in a positive light.
- Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues. We will only use images of pupils who are suitably dressed.
- We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk'.

### **Media Consent Form Agreement:**

I confirm that I have read and understood all school terms and conditions and that I agree to abide by their use.

**Name of the Student:** .....

**Name of the Parent:** .....

**Signature:** .....

**Signature:** .....

**Date :** \_\_\_\_\_

**Policies Implementation:** MARCH 2020

**First Review Date:** JANUARY 2021

**Second Review Date:** APRIL 2022

**Next Review Date:** JANUARY 2023





# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL ACCEPTABLE USE POLICY  
2022 - 2023**

## Overview

The use of information technologies and IT media has become integral to everyday life in modern society. At Al Ameer School, we use IT on a daily basis to enhance student learning in many diverse ways, both directly and indirectly. As a school, our role is not only to use and to teach our students to use these technologies, but also to educate the members of our community in how to use them safely and appropriately.

## Scope

The purpose of this Policy is to:

1. safeguard all students and staff;
2. provide guidance for students, staff and parents on the appropriate use of information technologies and media;
3. Provide a balance to support innovation within a framework of good practice, prevent or address potential inappropriate use of social media and social networking sites;
4. Protect the school from legal risks and ensure that the reputation of the school and its staff is protected.

This Policy should be read in conjunction with:

- Al Ameer Staff and Student Handbooks;
- Al Ameer' Positive Behavior, Safeguarding, Staff Conduct and Concerns & Complaints Policies;
- Al Ameer's Data Protection Policy.

## General Policy Statements:

**(With Expectations)**

### **I. TEACHERS**

are responsible for ensuring that:

1. They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
2. They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).

3. They report any suspected misuse or problem to the Supervisor / Principal /Vice Principal/ Academic Coordinator/ Curriculum Head; E-Safety Coordinator / Officer for investigation / action / sanction.
4. All digital communications with students / pupils / parents / guardians should be on a professional level and only carried out using official school systems.
5. E-safety issues are embedded in all aspects of the curriculum and other activities.
6. Students / pupils understand and follow the e-safety and acceptable use policies.
7. Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
8. They 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.
9. In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
10. Of the safe keeping of personal data, minimizing the risk of its loss or misuse.
11. Transfer data using encryption and secure password protected devices.
12. Use sensible email addresses and username. Use privacy settings and strong passwords.
13. Don't put anything online you wouldn't want your colleagues, family and friends to see.
14. Carefully consider if you want to connect with students or parents on social media.
15. Teachers should create an awareness on good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

16. Teachers have to select a digital ambassadors and techno Savvy, have to maintain a logbook of incidents during e-learning classes.

## **II. STUDENTS / PUPILS:**

are responsible-

1. For using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy.
2. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
4. Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
5. Should understand the importance of adopting good e-safety practice 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.
6. Students may not post personal information such as their home address, telephone number or the name and location of their school without teacher's permission.
7. Students are prohibited from making prejudicial, harassing, threatening, obscene or hateful remarks and other anti-social behavior.
8. Students are prohibited from using the Internet to access or process inappropriate text files, information that advocates illegal acts, or information that lacks any educational value.
9. Students should immediately tell a teacher or other school employee about any material that you feel is not appropriate or that makes you feel uncomfortable.
10. Students should be aware that no communications are guaranteed to be private. School portal use is monitored. Illegal activities may be reported to the authorities.
11. Students should note that plagiarism is the taking of material created by others and presenting it as if it were one's own. It will not be acceptable to plagiarize material from the Internet or from the portal.

12. Students should note that all communications and information accessible via the school portal should be assumed to be private property.
13. Students may not use the google classrooms or school portal for commercial purposes or product advertisement. Products or services may not be purchased or offered. The student and his/her parents will be responsible for any liabilities stemming from such unauthorized uses of the portal.
14. Student username and passwords are confidential. All passwords shall be protected by the user and not shared or displayed. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
15. Students may not send broadcast email or broadcast voicemail without prior permission from the Teacher.
16. Students are expected to check their email on a frequent and consistent basis in order to stay current with school related communications.
17. Students who violate school policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.
18. Students should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from Sharing of personal data, access to illegal / inappropriate materials inappropriate on-line contact with adults, strangers, potential or actual incidents of grooming, Cyberbullying.

### **III. PARENTS / GUARDIANS**

Parents / Guardians play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and guardians will be encouraged to support the school in promoting good e-safety practice and to follow guidelines:

1. On the appropriate use of digital and video images taken at school events.
2. Usage of access to parents' sections of the website / VLE and on-line student / pupil records.
3. Place the computer or laptop in a common area in your home within your supervision. This will allow you to indirectly monitor your child.

4. Frequently check the information being exchanged between your child their peers and the school on the third entity.
5. If you witness any inappropriate activity on an online platform, report immediately.
6. Install parental control software to block inappropriate content and websites that are not required for distance learning.
7. Follow the virtual timetables for your child.
8. Maintain regular family routines including bed time.
9. Student username and passwords are confidential. All passwords shall be protected by the user and not shared or displayed. Individual users shall, at all times, be responsible for the proper use of accounts issued in their name.
10. Parents may not send broadcast email or broadcast voicemail without prior permission from the Teacher.
11. Parents are expected to check their child's email on a frequent and consistent basis in order to stay current with school related communications.
12. Parents must be aware that if the child violates school policy or administrative procedures will be subject to suspension or termination of system/network privileges and will be subject to appropriate disciplinary action and/or prosecution.
13. Parents should monitor e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from Sharing of personal data, access to illegal / inappropriate materials inappropriate online contact with adults, strangers, potential or actual incidents of grooming, cyber-bullying.
14. Parents should be free to contact and acknowledge the issues faced by their ward if any during e-learning to the teacher concerned.

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**

# Acceptable Use Agreement

## Staff -Acceptable Use Policy -

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken -

Name of Staff : .....

Section : .....

Department : .....

Signed Date.....

\*\*\*\*\*

## Acceptable Use Agreement- Parents

### Parents/ Guidance Acceptable Use Policy Agreement:

- ☐ I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- ☐ I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's safety.

Name of Parent .....

Name of child/ children.....

Class & Division .....

Signed Date.....

\*\*\*\*\*

## Acceptable Use Agreement (G 9 To 12 Students)

**Kindly complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy (AUP) Agreement.**

This is how we stay safe when we use computers:

- ☐ I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- ☐ I will tell a teacher or suitable 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 my school Portal.

Name of Student / Pupil .....

Class & Division .....

Signed Date .....

\*\*\*\*\*

## **Acceptable Use Policy Agreement (Grd. 1 to 8)**

**Kindly complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy(AUP) Agreement.**

I have read and understand the above and agree to follow these guidelines when:

- ☐ I use the school Portal /systems (both in and out of school)
- ☐ I use my own id out of the school in a way that is related to me being a member of this school. E.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil .....

Class& Division .....

Signed Date .....

\*\*\*\*\*



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL CYBER BULLYING  
POLICY, 2022 - 2023**

## Scope

Al Ameer English School is committed to providing a safe and productive learning environment. Bullying of a student by another student is strictly prohibited on school property, in school buildings, on school buses, and at school sponsored events and/or activities whether occurring on or off campus.

### 1. Cyber Bullying

Cyber bullying is bullying takes place online. It can involve anything from sending messages to posting offensive comments to uploading and sharing private or embarrassing photos. It can take a number of different forms: threats and intimidation, cyber-stalking, sexting, defamation, peer rejection, and trolling. However, for those experiencing bullying behavior, the consequences can be just as serious and have far reaching effects.

## General policy Statements: -

Bullying is never acceptable and Al Ameer School fully recognizes its duty to protect all of its members and to provide a safe, healthy environment for everyone.

- Federal Law No. 3 of 2016 concerning child rights, also known as Wadeema's Law, stresses that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services and facilities without any kind of discrimination. The law protects children against all forms of negligence, exploitation, physical and psychological abuses.
- Federal Decree-Law No. (5) of 2012 on Combating Cyber-crimes
- Educational rights Article 32- Ban all forms of violence in educational institutions and maintain the dignity of the children upon taking decisions or setting programs.

## Roles and Responsibilities

Online Safety Group will take overall responsibility for the coordination and implementation of cyber bullying prevention and response strategies.

1. Ensure that all incidents of cyber bullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's Anti-Bullying Policy, Behavior Policy and Child Protection Policy.
2. Ensure that all policies relating to safeguarding, including cyber bullying are reviewed and updated regularly.

3. Ensure that all staffs report any concerns related to cyber bullying to Online Safety Leader.
4. Provide training to all parents, staffs and students on cyber bullying.
5. Ensure that all staffs, students and parents receive a copy of cyber bullying poster/leaflet.
6. Ensure that all students are given clear guidance on the use of technology safely, how to manage personal data, the risks associated with digital platforms and online harassments.
7. Provide annual training for parents and staffs on positive use of technology and online safety.
8. Ensure that all staffs are aware of their role in educating and supporting children who are affected by cyber bullying.

## **2. Guidance for Staffs**

- a. Ensure you understand your school's policies on the use of social media and Cyberbullying.
- b. Ensure you understand what is influencing the behavior of young people in your school community.
- c. Build confidence in dealing with incidents by continually updating your knowledge of safety procedures regarding online and offline incidents
- d. If you suspect or are told about a cyber-bullying incident inform the OSG immediately and pass them the information that you have
- e. Familiarize yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date.
- f. Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- g. Consider your own conduct online; certain behavior could breach your employment code of conduct
- h. Do not accept friend requests from students past or present
- i. Be aware that your social media friends may also be friends with pupils and their family members and therefore could read your post if you do not have appropriate privacy settings.
- j. Do not give out personal contact details
- k. Use your school email address for school business and personal email address for your private life

### **3. Guidance for Students**

Students who are victims of cyber bullying may feel so overwhelmed that they don't know what they can do about it. Following are some steps they can take to handle these situations and get the help they need.

1. Be careful who you allow to become a friend online and think about what information you want them to see.
2. Protect your passwords. Do not share it with anyone else.
3. Never reply to abusive mails and someone you don't know.
4. Do not give out personal information, location details without permission of a parent.
5. Record the dates and times when online bullying has occurred, and save and print screenshots, Emails and text messages
6. The student should block the bully on the platform and any other social media sites with which they are able to contact the victim.
7. Talk to a adult that you trust- Parents, Class teacher, Online Safety Group or any School staffs.

### **4. Guidance for Parents**

1. Parents can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
2. Parents should also explain to their children legal issues relating to cyber-bullying.
3. If parents believe their child is the victim of cyber-bullying, they should save the offending material.
4. Parents should contact the school as soon as possible.
5. Please contact Online Safety Leader Ms. Anjaly Sujith.
6. Parents should attend the school's annual training on online safety.
7. Parents should go through school portal and website for circulars, leaflet on cyber bullying policy and procedures

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL STUDENT'S BEHAVIOUR POLICY**

**2022 - 2023**

## General Policy Points

### **1<sup>st</sup> Degree Offences (Simple) Minor Behavioral Offences (Distance Learning) - 4 Marks will be detected**

1. A delay of (10) minutes or more from the beginning of a distance learning class when broadcasting live without an acceptable excuse.
2. Wearing clothes that violate public decency and morals while attending the period when broadcasting the distance learning period live.
3. Private conversations or discourse that are not related to study and hinder the course of the lesson during the live broadcasting of the distance learning period.
4. Ridiculing the teacher or a colleague during the distance learning period.
5. Eating while attending a distance learning period.
6. Adding any unauthorized program, including programs that are shared and free programs.
7. Using the microphone feature, camera or chat without prior permission from the teacher.
8. Playing games (except with the express permission of the teacher because it is an educational necessity linked to the lesson.)
9. Misusing rights and tools available through Microsoft Teams.

### **2<sup>nd</sup> Degree Offences (Medium Severity)**

### **Medium Severity Behavioral Offences (Distance Learning)- 8 marks will be detected**

1. Absence from a single school day (via distance learning) without an acceptable excuse.
2. Inciting students not to attend periods, threatening or intimidating them, and not attending periods in distance learning platforms.
3. Creating quarrels between students, whether visual or written, by broadcasting via synchronous and asynchronous distance learning platforms.
4. Not responding to the rules governing the course of lessons.
5. Misusing ministerial computers during or after the completion of distance education periods.
6. Engaging in audio and video communication with the rest of the students for non-educational purposes after the end of the official period time, be it on or off school premises.
7. Using e-mail or social media to reveal information of a personal nature.

8. Removing the teacher or students from the group that leads to blocking the course of the lesson, teacher's work and other students' rights.
9. Using profanity, racial slurs, or other language (text, sound, or hint) that may be offensive to any other user.
10. Abusing or insulting official visitors during periods during the live broadcast.

**3<sup>rd</sup> Degree Offences Serious Behavioral Offences (Distance Learning)- 12 Marks will be detected**

1. Using the initiative's communication and information technology to insult, curse, threaten with violence, slander, or blackmail in a deliberate and repeated manner via any digital platform.
2. Participating in unofficial mailing lists and bulletins within the distance education initiative and posting information about teachers and students without permission.
3. Posting about the initiative through social media.
4. Divulging other students' personal information, including home addresses and phone numbers.
5. Searching for information, obtaining specific copies, or modifying files and other data, or passwords belonging to other users on the network.
6. Entering and using the account of another teacher or student with or without his/her knowledge and/or consent.
7. Destroying, modifying, or misusing devices or software in any way.
8. Tampering, removing, requesting the removal of, or intentionally causing damage to any device, software or hardware.
9. Installing or downloading software or products that might harm the device or the network.
10. Using any camera (available as part of or as an add-on to certain devices) for personal use, and/or sharing photos or any information about any of the students' parents, employees, or any other person without their explicit consent.
11. Using educational content to photograph and recording conversations between students, and posting them without prior permission.

**4th Degree Offences (Very Serious) Very Serious Behavioral Offences (Distance Learning) – 20 Marks will be detected**

1. Creating or opening hyperlinks or any associated files unless they are sent from a trusted source.
2. Using montage software that can produce unreal and fake content and circulating it on social media.
3. Using the network to develop programs that harass users or to penetrate or destroy other people's accounts and devices.
4. Establishing networks or network connections to make live communications including audio or video (relay chat) without prior formal permission.
5. Publishing, creating, exchanging or promoting malicious or suspicious software.
6. Inundating e-mail accounts or applications used for distance education with high electronic data flow, stopping it them working, disabling them or destroying their contents.
7. Intentionally capturing or intercepting any communication without authorization through the information network used for distance education.

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**

## Section:

VP/PRINCIPAL:

## Section:

[illegible]

SIGN OF PRINCIPAL / VP:

## Section:

SIGN OF PRINCIPAL / VP:

**Section:**

SIGN OF PRINCIPAL / VP:

## Consolidation of Behaviour Management Distance Learning 2020 - 2021

NAME OF SUPERVISOR:

SECTION:

TERM:

Sl. No	Name of the student	Class & Div.	Total Score	Degrees of Offences								Score after Deduction	Supervisor s Awarding for Positive Behaviour	Supervisors Awarding for Exemplary Behaviour	Grand Total
				Simple ( 2+2)		Medium Severity ( 4+8)		Serious ( 12+12)		Very Serious ( 20+20)					
				80	1	2	1	2	1	2	1				
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
			80	0	0	0	0	0	0	0	0	80	0	0	80
Total				0	0	0	0	0	0	0	0	1120	0	0	1120

SIGN OF SUPERVISOR:

SIGN OF ACADEMIC CO ORDINATOR:

SIGN OF CURRICULUM HEAD:

SIGN OF VICE PRINCIPAL:

SIGN OF PRINCIPAL:



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL MANAGING MOBILE TECHNOLOGIES POLICY  
2022 - 2023**

## Overview

Mobile technologies offer opportunities for teaching and learning including a move towards personalized learning and 1:1 device ownership for children and young people. Mobile technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

### General policy Statements: -

#### Onsite class

1. There is a shared understanding of and adherence to the policy by all stakeholders and visitors and ensure increased vigilance.
2. The awareness of all staff is raised in their role of safeguarding in all areas of school life.
3. To ensure staff, pupils and parents are familiar with the school policy of pupil use of personal mobile technology in school.
4. To highlight the child protection issues of using camera and video phone technology in the school. To counter the use of text messaging as a form of bullying.
5. To determine exactly when and where mobile phone use is permitted in the school.
6. Offer safety guidelines to the pupils/staff on general mobile phone use.
7. To outline the consequences of not adhering to the school mobile technology policy.
8. To outline who has responsibility in the case of loss, theft or damage of mobile technology.

#### For Staff

1. Staff are reminded to familiarize themselves with the school's e-safety and acceptable use of IT policies which set out in further detail the measures needed to ensure responsible behavior online.
2. The school allows staff to bring in personal mobile phones and devices for their own use. Staff use of mobile devices must not hinder their working day and must not be used during class hours.
3. Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.
4. Class teachers are permitted to use mobile phones to mark the attendance using school app.
5. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
6. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
7. The sending of inappropriate text messages between any members of the school community is not allowed.

8. Staff can Access the following school IT services from their mobile devices:
  - a. The school email system
  - b. Official school apps.
9. School information accessed through these services is confidential, in particular information about pupils and staff. Staff must take all reasonable measures to prevent unauthorized access to it. Any unauthorized access to or distribution of confidential information should be reported to the school's Network Manager as soon as possible in line with the school's data protection policies

### **For Students**

Student mobile phone use is prohibited on the school site, including all social times and class changeover. This applies to any electronic device brought in by students that is deemed to be obstructive and disruptive to teaching and learning. This may include phones I- pods, DS/Gameconsoles and smart watches

- ❖ Students can bring personal mobile devices/phones to school must hand them into the office at the start of the day.
- ❖ Mobile technology must not be used to share inappropriate or offensive imagery or messages at any time.
- ❖ The school is not responsible for the loss, damage or theft of any personal mobile device.
- ❖ Students found with their phones or accessories out:
  - The phone is confiscated, and behavior for learning policy followed.
  - The phone is placed in office to be collected at the end of the day by the student.
  - Repeat offenders (two or more incidents), parents are to be contacted and are required to pick up the phone from student office when convenient with pastoral team informing parents and an escalation sanctioned if required
  - If the student refuses to hand the phone over, the school behavior policy is to be followed and pastoral team to follow up if escalation is required

### **Visitors (including parents, professionals, contractors):**

1. Visitors may bring mobile phones on to the school site but are asked to switch them off and place them out-of-sight until they leave exiting the school gates/reception.
2. Parents/carriers are permitted to take photos/videos during assemblies or other school performances that involve their own children. . They are reminded not to place photographs or videos showing other children on Face book or other social media platforms.

## **Emergencies:**

If parents need to contact pupils they should contact the school office and a message will be relayed promptly

## **Responsibility for mobile phones and other mobile devices:-**

The school accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile technology including any confiscated item. It is the responsibility of staff, parents, pupils and visitors to make sure that mobile technology is properly insured. The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network.

### **ACCEPTABLE USE POLICY (AUP) FOR DEVICES**

Communication Technologies	Staff				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones maybe brought to school	Yes				no			
Use of mobile phones in lessons	no				no			
Use of mobile phones in social time	yes				no			
Taking photos on mobile phones / cameras	yes						yes	
Use of other mobile devices eg tablets, gaming devices		yes			no			
Use of personal email addresses in school, or on school network	yes						Yes	
Use of school email for personal emails	yes					yes		
Use of messaging apps	yes				no			
Use of social media		yes			no			
Use of blogs	yes					yes		

### **Parent Agreement form**

I agree to follow the school's Acceptable Use Policy on the use of the Mobile Technology.  
I will use the devices in a responsible way and obey all the rules explained to me by the school.

Signature of Student\_\_\_\_\_

Date:

Signature of Parent/Guardian\_\_\_\_\_

Date:

### **Staff Agreement form**

I agree to follow the school's Acceptable Use Policy on the use of the Mobile Technology.  
I will use the devices in a responsible way and obey all the rules explained  
to me by the school.

Signature of Staff\_\_\_\_\_

Date:

## Online Class

Technology is an integral and essential part of the learning experience at Al Ameer English School. We are committed to ensure that our children leave with the skills and Knowledge that will assist them to thrive in our digital age. In this pandemic situation the schooling system shifted to online classes. It is therefore also vital that we teach children how to use this valuable resource safely.

To ensure the school's online procedures keep children and parents safe, we need to teach them about online safety, in and outside of school. This will appreciate that all children have access to smart phones, Ipads and computers at home. It promotes the use of these technologies whilst committing to keep our children aware of and safe from the potential risks. We try to foster an open environment in which children and parents are encouraged to ask any questions and participate in an ongoing conversation about the benefits and dangers of the online world. Our school has provided the necessary safeguards to ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

In order to empower teachers and students in this area our school arranging webinar to:




- ensure teachers have the knowledge to teach students about e-safety
- provide advice on using social media and other online related activities.
- support and include parents and students by sharing helpful advice and resources
- review and update your e-safety provision on an ongoing basis.

So, as the first step our school conducted one webinar for the teachers by our Vice Principal, E-safety team leader. We have scheduled more webinars for teachers children and parents. Online safety information is clearly published on the school website and available for all users.

## Handling online-safety concerns and incidents:

- It is vital that all staff recognize that online-safety is a part of safeguarding.
- Any suspected online risk or infringement should be reported to the online safety lead /designated safeguarding lead on the same day of the incident reported.
- School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber bullying.
- Social media incidents are handled by school behavior policy
- Appropriate filtering and monitoring systems are in place to ensure no inappropriate materials are not accessed by students.
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the OSL or other member of the senior leadership team to decide whether they should:
  - Delete that material, or
  - Retain it as evidence

## Sample Incident Reporting Logbook:

<div>    </div> <div>Open with Google Docs</div>										
E-SAFETY INCIDENT LOG BOOK										
Sl no	Name of person reporting incident:	Date and time of incident:	Date incident reported:	Names of people involved:	Class & Division	Location and device details:	Details of incident, including evidence:	Clarification of the risk or breach e.g. does it relate to safeguarding, bullying, inappropriate content, data protection, copyright, infringement, sexting, etc?	Initial action taken and current status:	Resolution of incident:
1	Mrs. Sheena	4/10/2020 8:10 AM	9/10/2020	Fathima Hameema	12B	12B EXAMROOM	Her Laptop got stuck when she started loom recording. Started the exam late but could complete on time	Device issue	Reported to Supervisor & IT head	
2	Mrs. Ashely	4/10/2020 11:10 AM	4/10/2020	1. Fathima Shirin 2. Meenakshi	12B	12B EXAMROOM	Shirin faced data loss in google form as she is using mobile to write the exam. Meenakshi lost the content due to slow network	Data Loss	Reported to Supervisor & IT head	
3.	Mrs. Sajeena	9/10/2020 11.00AM	9/10/2020	Amina	12B	12B EXAMROOM	Loom recording was missing as she repeated the exam due to network problem	Data Loss	Reported to Supervisor	

### Report on Hr. Sec. Students Online safety Issues

Sno	Name of the student	class	Reason	Actions taken	Follow up
1	Nabila Mehak	XII D	Social media addiction/Game Addiction	Referred to the school counselor	Informed the matter to the parents.
2.	Adithyan Biju	12C	Social media addiction	Referred to the school counselor	Encouraged the parent to have a friendly talk with child.
3	Satyam Nayak	12C	Game Addiction	Referred to the school counselor	Asked them to monitor the online activities .Ensure their participation in various school activities such as Assemblies & Talents day program .

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**

## **E-SAFETY INCIDENT REPORT FORM**

*This form should be kept securely in file.*

### **DETAILS OF INCIDENT**

**Reporting Date :**

**Date of Incident :**

**Time of Incident :**

**Name & Designation of Person Reporting Incident**

**Where did the incident occur?**

Inside the School ☐

Outside the School ☐

**Who was involved in the incident?**

Student ☐

Staff Member ☐

Other (Please Specify) :

**Name & Details of Persons/Students Involved**

**Type of incident :**

Cyber Bullying / Harassment ☐

Deliberately bypassing Security or Access ☐

Accessing unsuitable contents in Internet ☐

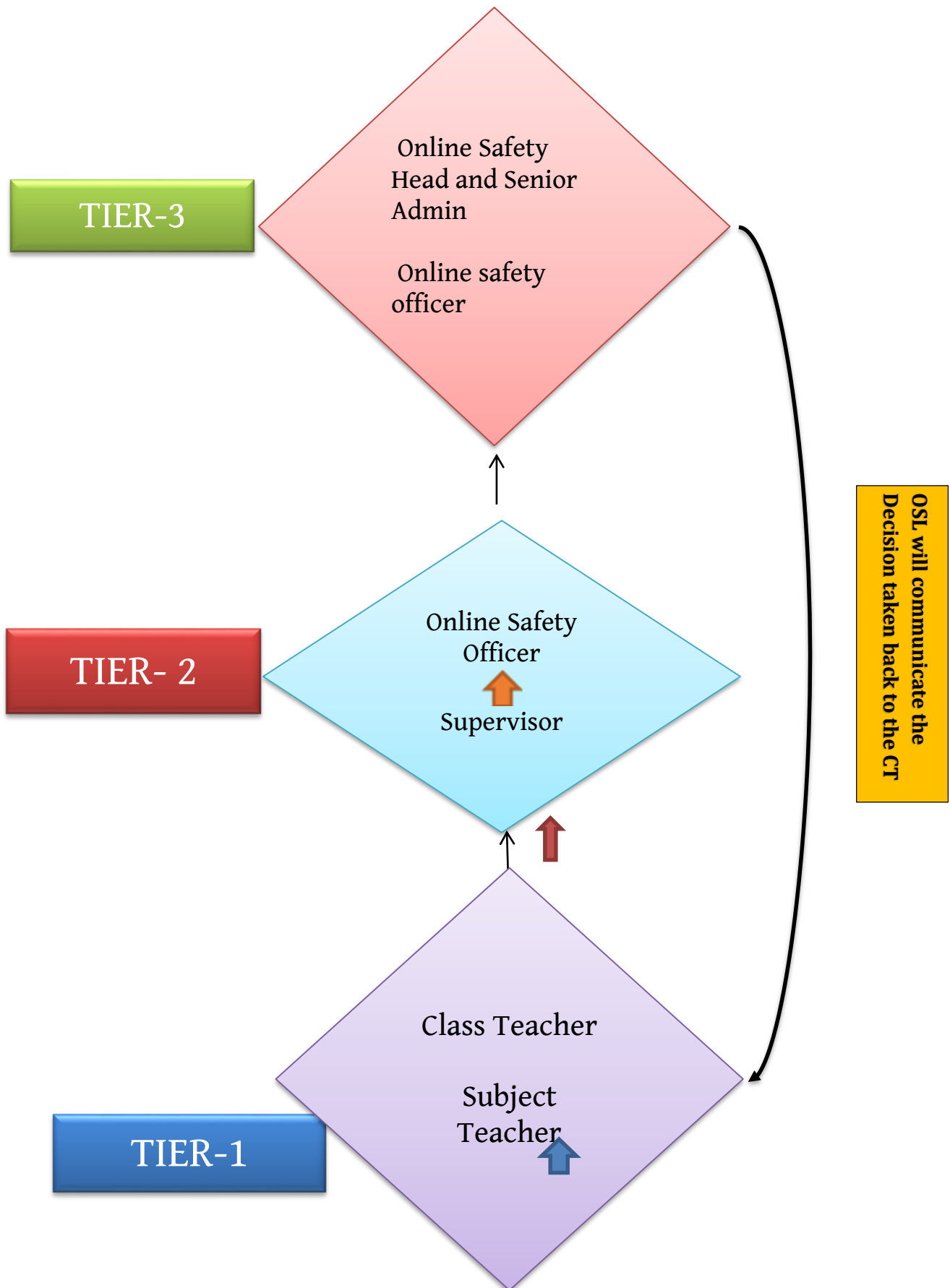
Racist/ Religious hate materials ☐

Extremism ☐

Materials of Sexual Nature ☐

Others ( Please Specify ) :

## Communication plan for incident reporting





# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL MANAGING DIGITAL CONTENT POLICY  
2022 - 2023**

## Overview

# “A child’s Online Safety is Nation’s Responsibility”

Members of the Managing Digital Content in E-safety Group will assist the E-Safety Officer (or other relevant person, as above) in:

- Developing a **separate wing for E-safe resource** in E-safety platform
- Displaying /publishing / monitoring the **school e-safety policy / documents**.
- Designing/ Managing / formulating **e-safety library** by including various means to learn about their favorite app (Eg: Word search, City/nature/school campus coloring in a sheet by including one or two questions about their favorite app or games, etc.)
- Developing / designing and publishing **hashtag cautionary tale and E-safety tips for children** in order to make them aware about their internet activities
- Designing **guidelines for parents and teacher** to have a friendly and natural conversation with your children about online safety
- Publishing **e-safety posters, presentations, videos and various useful documents for children** of different age group, teachers, staffs and parents.
- Providing **various website links for parents** to keep children safe at home.
- Collecting and displaying all the **online safety issues and solutions** in E-safe resources
- Filing and Publishing **school based E-safe activities** which have been conducted for children, parents, teachers and staffs.
- Images and Videos: **written consent from parents to publish images or videos** for any external publicity purposes. Parents and guardians may withdraw their permission at any time by informing the administration team in writing.
- Digital technology agreement in addressing the risks by Children.

## General policy Statements: -

### **GUIDELINES /TIPS FOR STAYING SAFE ONLINE DURING THE COVID 19 PANDEMIC**

Due to school closings and stay-at-home orders resulting from the COVID-19 pandemic, children's increased online presence may put them at greater risk of child exploitation. Parents, guardians, caregivers, and teachers can take the following measures to help protect children from becoming victims of online child predators.

**Discuss internet safety and develop an online safety plan** with children before they engage in online activity. Establish clear guidelines, teach children to spot red flags, and encourage children to have open communication with you.

**Supervise young children's use of the internet**, including periodically checking their profiles and posts. Keep electronic devices in open, common areas of the home and consider setting time limits for their use.

**Review games, apps, and social media sites** before they are downloaded or used by children. Pay particular attention to apps and sites that feature end-to-end encryption, direct messaging, video chats, file uploads, and user anonymity, which are frequently relied upon by online child predators.

**Adjust privacy settings and use parental controls** for online games, apps, social media sites, and electronic devices.

**Tell children to avoid sharing personal information, photos, and videos online** in public forums or with people they do not know in real life. Explain to your children that images posted online will be permanently on the internet.

**Teach children about body safety and boundaries**, including the importance of saying 'no' to inappropriate requests both in the physical world and the virtual world.

**Be alert to potential signs of abuse**, including changes in children's use of electronic devices, attempts to conceal online activity, withdrawn behavior, angry outbursts, anxiety, and depression.

**Encourage children to tell parents, guardian, or other trusted adult** if anyone asks them to engage in sexual activity or other inappropriate behavior.

## Social Media Guidelines

Social media refers to online tools and services that allow any Internet user to create and publish content. Social media allows those with common interests to share content easily, expanding the reach of their ideas and work. Popular social media tools include Face book, Twitter, LinkedIn, blogs, YouTube and Flickr to name a few. **Students: Social Media Guidelines:**

1. Not join any social networking sites if they are below the permitted age (13 for most sites including Face book and Instagram)
2. Not access social media on school devices, or on their own devices while they're at school
3. Inform parents when they are online.
4. Think before you post. To use discretion when posting to the internet.
5. School-related images or content posted without permission to be removed from the internet.
6. Do not misrepresent yourself by using someone else's ID.
7. Users should keep their passwords secure and never share passwords with others. If someone tampers with your blog, email, or social networking account without you knowing about it, you could be held accountable.
8. Cyber bullying is considered an act of harassment.
9. When responding to others, remember to be respectful and avoid comments that may be hurtful. Do not use profane, obscene, or threatening language.
10. Only accept invitations to share information from people you know. Utilize may do so only by means of a link to the official School's Face book account, or Twitter account.

### **Faculty & Staff: Social Media Guidelines:**

1. Higher authority should provide opportunities to discuss appropriate social networking use by staff on a regular basis and ensure that any queries raised are resolved swiftly and should ensure there is a system in place for regular monitoring.
2. School staff should ensure that they are familiar with the contents of this policy and its relationship to the school's standards, policies and guidance on the use of ICT and e-safety and must comply with this policy where specific activities or conduct is prohibited.
3. Staff **must not** place a child at risk of harm.
4. Staff **must** follow statutory and school safeguarding procedures at all times when using social media.
5. Staff **must** report all situations where any child is at potential risk by using relevant statutory and school child protection procedures
6. Staff **must** maintain the reputation of the school, its staff, its parents, its wider community and their employers.

7. Staff **must not** use social media to criticize or insult their school, its staff, its parents, or its wider community.
8. Staffs are responsible for their actions (and its consequences) whenever they use social media.
9. Staff **must** be given explicit permission to use social media on behalf of their school by a school leader.
10. Staff must not reveal any other private or confidential school matters when using any social media.

### **Parents: Social Media Guidelines:**

1. Parents should expect communication from teachers prior to their child's involvement in any project using online social media applications, i.e., Facebook, blogs, etc.
2. Parents will need to sign a release form for students when teachers set up social media activities for classroom use.
3. Parents will not attempt to destroy or harm any information online.
4. Parents will not use classroom social media sites for any illegal activity, including violation of data privacy laws.
5. Parents are highly encouraged to read and/or participate in social media.

## **Social Media Consent Form**

**Dear Parents,**

School websites and some digital services provide schools with excellent opportunities to broadcast their achievements to a wide audience. Details of the school, its curriculum and its facilities can and do provide a showcase for the activities of staff and pupils. As part of our school activities, we may occasionally take photographs or videos of the children. These could be individually or in groups. We use these to record achievement and to celebrate those achievements within the school.

**However, we also may wish to use these images in many other ways:**

- school website ➤ school displays
- school publicity material
- school newsletter
- local or national media
- Face book page

**On the attached Consent Form:** We will ask for your consent for

- The school to take digital images or videos of your child.
- Digital images or videos of your child to be used on the official school web site.
- Digital images or videos of your child to be used on the school's official Face book page.
- Digital images of your child to be used in the school promotional material for the school, such as flyers and leaflets.
- Digital images or videos of your child to be used in internal displays.
- Digital images or videos of your child to be taken when involved in school events, such as a Sports Day. The school may make these images or videos available to other parents.

## **Parent Consent Form**

Please complete and return: -

Child's name:	
Class & Division :	

Type of Consent	Yes	No
I give consent for the school to take digital images and videos of my child		
I give consent for the school to mention the name or any other required details of my child to be used on the official school web site or official Face book page.		
I give consent for digital images of my child to be used on the official school web site.		
I give consent for digital images of my child to be used on the school's official Face book page.		
I give consent for digital images of my child to be used in the school prospectus and other promotional material for the school, such as flyers and leaflets.		
I give consent for digital images of my child to be used in internal displays.		
I give consent for digital images of my child to be taken when involved in school events; such as Assemblies, Sports Day etc. The school may make these recordings available to other parents.		

I hereby agree to the Schools terms and conditions especially regarding the use of social media. I accept that I will be held responsible where any images I may have shared with others (e.g. family members) are uploaded to social media.

Name &Signature of the parent:

## **Terms and Conditions**

This form is valid for the period your child attends this school. Images of your child will not be used after this time.

1. Please write to the school if you wish to withdraw consent at anytime.
2. The images we take will be of activities that show the school and children in a positive light.
3. Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues.
4. We may use group or class photographs or footage with very general labels e.g. 'science lesson'.
5. We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk' or disallowed from having their photographs taken for legal or social reasons.
6. We will take all reasonable measures to ensure the images are used solely for the purposes for which they are intended. However, we cannot guarantee this and take no responsibility for the way images are used by other websites or publishers or for any consequences arising from publication.

*Once your child leaves the school, this form will be considered invalid and if we would like to continue to use your child's image (e.g. in publicity material) we will obtain renewed, written consent.*

## Digital technology agreement for Students on Online Safety

There are some risks in using digital technology – follow these advice and sign this agreement to help you to keep safe.

### Advice:-

- ✓ Be careful what information you put on the internet and who can see it. Use a nickname online and privacy settings. This can help keep you safe.
- ✓ Don't give personal information like email address, home or school address or mobile phone number to people you do not know.
- ✓ Only post photographs which you should be happy with your parents/careers seeing and make sure they don't show address. Photographs you post can be copied and sent to other people meaning you are not in control of them.
- ✓ Do not share your passwords and log in details as people could access your information without your permission.
- ✓ Change your passwords frequently.

I agree;

- ☒ I agree not to access sites that are inappropriate for my age or download inappropriate content and I will tell adults about the sites that I am worried about.
- ☒ I agree to report any unpleasant experience to an adult.
- ☒ I agree not to send rude or pornographic pictures or videos (often called sexting) ☒ I agree not to use any digital technology to bully people or make threats.

Name:

Class & Division:

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**RESOURCES :-**

<b>Content</b>	<b>Beneficiary</b>	<b>Links</b>
<b>Goldilocks (a Hashtag Cautionary Tale)</b>	Children	<a href="https://books.google.ae/books?id=A_9PxQEACAAJ&amp;dq=editions:9_EtGj4HBt4C&amp;hl=en&amp;sa=X&amp;ved=2ahUKEwiri82SybTsAhUUiFwKHQ-zCSgQ6AEwAHoECAAQAg">https://books.google.ae/books?id=A_9PxQEACAAJ&amp;dq=editions:9_EtGj4HBt4C&amp;hl=en&amp;sa=X&amp;ved=2ahUKEwiri82SybTsAhUUiFwKHQ-zCSgQ6AEwAHoECAAQAg</a>
The service works for: All children of all nationalities under the age of 18 residing in Dubai in order to bring up happy, safe and empowered children who are aware of their own rights.	<b>Abused children and their Family</b>	<b>Official website of UAE government</b> <a href="https://www.cda.gov.ae/en/socialcare/childrenand youth/Pages/ChildProtectionCentre.aspx">https://www.cda.gov.ae/en/socialcare/childrenand youth/Pages/ChildProtectionCentre.aspx</a>
The UAE protects children by enforcing laws to protect them and empowers them by providing education, good health and other facilities	<b>Abused children and their Family</b>	<b>The United Arab Emirate's Government Portal (children's safety )</b> <a href="https://u.ae/en/information-and-services/justice-safetyand-the-law/children-safety">https://u.ae/en/information-and-services/justice-safetyand-the-law/children-safety</a>
<b>GUIDELINES FOR PARENTS TO SUPPORT THEIR CHILDREN DURING DISTANCE LEARNING</b>	ADEK'S PARENT GUIDE FOR DISTANCE LEARNING	<a href="https://adek.gov.ae/-/media/Project/TAMM/ADEK/Health/ADEKPARENT-GUIDE.pdf">https://adek.gov.ae/-/media/Project/TAMM/ADEK/Health/ADEKPARENT-GUIDE.pdf</a>


Awareness classes and webinars by National Online Safety team	Students & Parents	<a href="https://nationalonlinesafety.com/hub/online-copyrightownership">https://nationalonlinesafety.com/hub/online-copyrightownership</a>  <a href="https://nationalonlinesafety.com/hub/social-media">https://nationalonlinesafety.com/hub/social-media</a> <a href="https://nationalonlinesafety.com/hub/view/webinar/digital-footprint">https://nationalonlinesafety.com/hub/view/webinar/digital-footprint</a> <a href="https://nationalonlinesafety.com/hub/view/webinar/identity-theft">https://nationalonlinesafety.com/hub/view/webinar/identity-theft</a> <a href="https://nationalonlinesafety.com/hub/view/webinar/digital-manipulation">https://nationalonlinesafety.com/hub/view/webinar/digital-manipulation</a>  <a href="https://nationalonlinesafety.com/hub/onlinerelationships">https://nationalonlinesafety.com/hub/onlinerelationships</a> <a href="https://nationalonlinesafety.com/hub/view/webinar/hacking">https://nationalonlinesafety.com/hub/view/webinar/hacking</a>  <a href="https://nationalonlinesafety.com/hub/privacy-andsecurity?page=2">https://nationalonlinesafety.com/hub/privacy-andsecurity?page=2</a>
---	--------------------	--











Page 9 of 18

# ESAFETY TIPS FOR CHILDREN POSTED IN SCHOOL WEBSITE AND VIRTUAL PLAT

## FORM

### Online Safety Tips: 10 tips for staying safe online



<b>PUT A PIN IN IT</b> Whether it's a phone, website or a social media account, your first line of defence is a PIN or Password. Never use the same password, make sure it is hard to guess (don't use your pet's name, your birthday or your favourite football team) and never share your passwords with anyone.		<b>BE SOFTWARE SAVVY</b> Protect all your devices with security software and make sure you regularly install updates to any programs or apps, as they often include improved security settings.	
<b>LOOK FOR THE PADLOCK</b> When shopping or banking online always check there is a padlock symbol in the web browser window when you have logged in or registered, and that the web address begins with 'https://'. The 's' stands for 'secure'.		<b>POST IN HASTE, REPENT AT LEISURE</b> What goes online stays online so never say anything that could hurt, anger or endanger yourself or someone else.	
<b>SECURE THE WIFI</b> Make sure your home WiFi is protected with a strong password that only you and your family know. When out and about never use a hotspot that may be unsecured, especially when what you're doing is personal or private.		<b>KEEP IT PRIVATE</b> Check the privacy settings on all of your social media accounts so that only the people you want to share your information with can see it.	
<b>LOG-OUT/LOG-OFF</b> Always make sure you log out of your accounts when you've finished with them and log off a computer when you've finished using it.		<b>BID SMARTLY</b> When using an auction site, make sure you never transfer any money directly to a bank account or hand over any personal details. If you're thinking of making a big purchase like a car, or finding somewhere to live, always make sure it exists and is genuine.	
<b>MANAGE YOUR MESSAGES</b> Never open or forward a suspicious looking email, or respond to a social media message from someone you don't know.		<b>REPORT IT</b> If you are a victim of online fraud, report it to <a href="http://www.actionfraud.police.uk">www.actionfraud.police.uk</a> , this way we can all help to make the internet a safer place.	

Children and adults using an Internet or computer network, or any other means of communication, should be aware of the information they receive and the people they interact with. It is important that children and adults are aware of the information they receive and the people they interact with. It is important that children and adults are aware of the information they receive and the people they interact with.

There are many reasons why children and adults should be aware of the information they receive and the people they interact with. It is important that children and adults are aware of the information they receive and the people they interact with. It is important that children and adults are aware of the information they receive and the people they interact with.

# Do Video Games Actually Cause VIOLENT BEHAVIOUR?

FOR AGAINST

## VIOLENT AND MATURE THEMES

There's no denying that video games can contain violent and mature themes. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

Similarly, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## ANGER EXHIBITED DURING OR AFTER PLAYING GAMES

It's not uncommon for children to get angry or frustrated while playing video games. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

In 2011, a study by the American Psychological Association (APA) suggested that video games can cause anger and aggression. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## RELATIVELY UNKNOWN LONG-TERM EFFECTS

While there are many studies on the effects of video games, there is still a lot of uncertainty about the long-term effects. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## HISTORICAL HYSTERIA

Historical hysteria is a term used to describe the fear of video games in the past. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

The history of video games is full of controversy. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## ALMOST EVERY MODERN SCIENTIFIC STUDY

Almost every modern scientific study has found that video games can cause anger and aggression. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

In 2011, a study by the American Psychological Association (APA) suggested that video games can cause anger and aggression. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## MISUNDERSTOOD OUTSIDE FACTORS

Many people believe that video games are the cause of violent behavior. However, it's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

There are many other factors that can contribute to violent behavior. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.



## SHOULD WE STOP BLAMING VIDEO GAMES FOR VIOLENT AND AGGRESSIVE BEHAVIOUR?

Blaming video games for violent and aggressive behavior is a common mistake. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

## Meet our expert

Dr. David Anderson is a leading expert on the effects of video games. He has written many books and articles on the topic. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.



Dr. Anderson is a leading expert on the effects of video games. He has written many books and articles on the topic. It's important to remember that video games are a form of entertainment, not a source of information. It's up to parents to decide if their child is ready for the content.

www.nationalonlinesafety.com Twitter: @natonsafety Facebook: /NationalOnlineSafety

Version of this guide is available on the website. The full guide is available on the website. The full guide is available on the website.

Without Online Safety we believe everyone's access to the information they need to be an informed consumer and to be safe with their children, should be in a state of need. This guide focuses on our platform of simple, achievable, and effective advice to help you and your children be safe online.



# 14 WAYS TO BE KIND ONLINE

Being kind online can mean so much to someone else. It is a choice we can all make that helps others, puts people's needs before our own and which can generate feelings of empathy and compassion. So, everyone can have a big impact and often we act of kindness can lead to more, making the world a happier and more positive place. That's why we've created this guide to suggest a few simple 'acts of kindness online' that can benefit people's mental health, support their wellbeing and encourage a more positive approach to engaging online.



## 1. BE POSITIVE

If somebody says something that you like on social media, like a post or a video, it's a good idea to let them know you like it.



Even if you're a friend or family member, it's good to offer to help someone who is struggling. If you know the answer to an online offer to help, please accept and send a response. Something that may be easy for you might be difficult for someone else.



If somebody you know has done something good to help someone else, thank them for it. It's a good idea to let them know that you appreciate it.

## 4. SHARE FUNNY VIDEOS OR IMAGES WITH FRIENDS & FAMILY

We often come across funny videos or images online that make us laugh and that we want to share with our friends and family. It's a good idea to share them with them. It could help someone else who may be having a bad day.



## 8. SHARE POSITIVE POSTS

If you see something online that inspires you, shares a useful tip or a beautiful quote, it's a good idea to share it with your friends and family. It could help someone else who is struggling.

## 6. VIDEO CALL YOUR FRIENDS & FAMILY

It's a good idea to be connected by video call. It's a good idea to be connected by video call. It's a good idea to be connected by video call.



## 7. TELL SOMEONE YOU'RE THINKING OF THEM

We often forget to tell our friends and family that we're thinking of them. It's a good idea to tell them that we're thinking of them. It could help someone else who is struggling.

## 9. HOST AN ONLINE QUIZ

When you have a quiz, it's a good idea to host it online. It's a good idea to host it online. It's a good idea to host it online.

## 10. THANK BEFORE YOU COMMENT

When you're thinking about commenting on a post, it's a good idea to thank the person who posted it first. It's a good idea to thank the person who posted it first.

## 11. BE COMPASSIONATE & UNDERSTANDING

Being compassionate and understanding is a good idea. It's a good idea to be compassionate and understanding. It's a good idea to be compassionate and understanding.

## 12. CONNECT FRIENDS & FAMILY WITH SIMILAR INTERESTS

It's a good idea to connect friends and family with similar interests. It's a good idea to connect friends and family with similar interests.



## 13. RECOMMEND SOMETHING YOU ENJOY DOING TO OTHERS

If you enjoy doing something online, it's a good idea to recommend it to others. It's a good idea to recommend it to others.



## Meet our expert

Therapist and author of the book 'The Art of Being Kind' is a good idea. It's a good idea to be kind. It's a good idea to be kind.



## 14. PRAISE OTHERS FOR THEIR ACHIEVEMENTS

It's a good idea to praise others for their achievements. It's a good idea to praise others for their achievements.

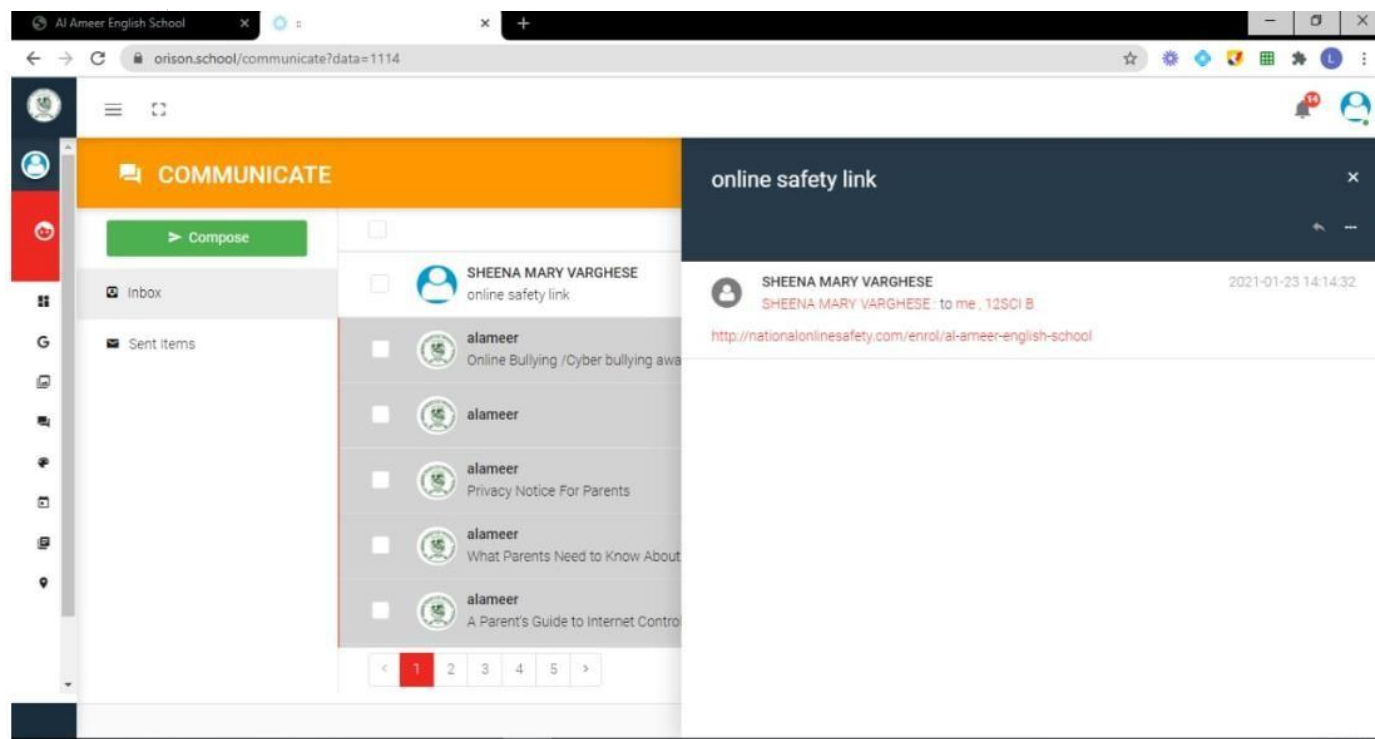


www.nationalonlinesafety.com Twitter: @nationalonlinesafety Facebook: NationalOnlineSafety Instagram: @NationalOnlineSafety

Version 1.0 published on 15th March 2021. All rights reserved. No part of this publication may be reproduced without prior permission.



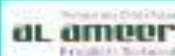
## ONLINE COMMUNICATION THROUGH SCHOOL MAILING SYSTEM



## SOCIAL MEDIA AWARENESS SURVEY CONDUCTED FOR CYCLE 3 STUDENTS

Survey Link :- <https://forms.gle/pGzaP2ydunhFyjQD8>

Name of the student	Class & Division	1. how many social media apps do you use	2. how much time do you spend on social media	3. how often do you post on social media	4. if you have been talking to someone on social media, how often do you talk to them	5. Does your school give a lesson on digital footprint?	6. What is a Digital Footprint?	7. Are you aware of Identity Theft?	8. VR
Fathima diya	11d	2	less than 30 minutes	weekly	Ask your parent or guardian	Yes	Credit Card and Check information	Yes	Being
Fathima Iamiya	11 D	1	less than 30 minutes	never	Ask your parent or guardian	Yes	A digital image of your face	Yes	Being
Goury Rajeev	12 B	1	less than 30 minutes	monthly	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Lubaiba	11 D	More than 3	3 hours +	weekly	Ask your parent or guardian	Yes	Only what you post on social media	Yes	Being
Shredha anil	11 d	More than 3	30-60 minutes	monthly	Ask your parent or guardian	Yes	A digital image of your face	Yes	Being
adithyan r prince	12 a	2	less than 30 minutes	monthly	Ask your parent or guardian	Yes	Credit Card and Check information	Yes	Being
Jaishnavy Dev Sajeev	10&D	More than 3	2-3 hours	never	Ask your parent or guardian	Yes	Only what you post on social media	Yes	Being
sharifa	10d	1	2-3 hours	never	Meet them, as long as you want	Yes	Past and present statements	Yes	None
Athul Antony	10 c	0	less than 30 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Ashwini Jayan	12 B	1	30-60 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Azna Mujeeb	11B	1	less than 30 minutes	monthly	Ask your parent or guardian	Yes	Past and present statements and images you post	Yes	Being
Imran noor	9 A	More than 3	30-60 minutes	never	Tell someone where you are	Yes	A digital image of your face	Yes	Being
JERIN JOHN KUTTY	12-A	1	30-60 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Mohammed shareef	10-E	1	30-60 minutes	monthly	Ask your parent or guardian	Yes	Past and present statements	Yes	Shari
Levina Merin Sharly	11 B	3	30-60 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Soorya Kiran Kakkarayil	10-E	1	2-3 hours	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Ahmed Hakimji	10 E	1	30-60 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
SADIA AKBAR	11 B	1	less than 30 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Muhammed Hilal	10-E	2	30-60 minutes	never	Meet in a public place	Yes	Past and present statements	Yes	Secu
Anand Parayil Sunil Kum	10 E	0	less than 30 minutes	never	Ask your parent or guardian	Yes	Past and present statements	Yes	Being
Nuha Nafeesa	10-D	2	2-3 hours	never	Ask your parent or guardian	Yes		Yes	Being



# Orange Education Presents Webinars on **E-SAFETY GUIDELINES**



## WEBINAR 1

### FOR STUDENTS

Sunday 18th October  
4 pm – 5 pm

**TOPIC: Staying Safe Online**

04:00 pm – 04:15 pm  
*Dr. Seema Negi*

**TOPIC: Cyber Bullying**

04:15 pm – 04:30 pm  
*Ms. Shivani Sahni*

**TOPIC: Tips for Safe  
Internet Usage**

04:30 pm – 04:45 pm  
*Ms. Shivani Sahni*

**Q/A Session**

04:45 pm – 05:00 pm

## WEBINAR 2

### FOR TEACHERS

Thursday 22nd October  
4 pm – 5 pm

**TOPIC: Current Cyber Safety  
Trends & Risks**

04:00 pm – 04:15 pm  
*Mr. Saurabh Maheshwari*

**TOPIC: Supporting  
Students Online**

04:15 pm – 04:30 pm  
*Mr. Saurabh Maheshwari*

**TOPIC: Staying Safe Online**

04:30 pm – 04:45 pm  
*Dr. Seema Negi*

**Q/A Session**

04:45 pm – 05:00 pm

## WEBINAR 3

### FOR PARENTS

Friday 23rd October  
4 pm – 5 pm

**TOPIC: Setting up a  
Cyber Safe Home**

04:00 pm – 04:20 pm  
*Dr. Seema Negi*

**TOPIC: Parenting in  
Digital World**

04:20 pm – 04:40 pm  
*Dr. Seema Negi*

**Q/A Session**

04:40 pm – 04:45 pm

## MODERATOR



**Ms. Nidhi Gupta**  
Educationist & Author  
Editorial Manager,  
Orange Education

## THE EXPERT PANELISTS



**Dr. Seema Negi**  
Principal  
Sanjeevani World School,  
Global Goodwill Ambassador  
Life Coach



**Ms. Shivani Sahni**  
Educational Leader,  
Delhi



**Mr. Saurabh Maheshwari**  
National Trainer

## Evidences for Parent Consent form



### Parent Consent Form

Please complete and return: -

Child's name:	Naina Santosh
Class & Division:	TD

Type of Consent	Yes	No
I give consent for the school to take digital images and videos of my child	✓	
I give consent for the school to mention the name or any other required details of my child to be used on the official school web site or official Face book page		✓
I give consent for digital images of my child to be used on the official school web site	✓	
I give consent for digital images of my child to be used on the school's official Face book page	✓	
I give consent for digital images of my child to be used in the school prospectus and other promotional material for the school, such as flyers and leaflets	✓	
I give consent for digital images of my child to be used in internal displays	✓	
I give consent for digital images of my child to be taken when involved in school events, such as Assemblies, Sports Day etc. The school may make these recordings available to other parents	✓	

I hereby agree to the Schools terms and conditions especially regarding the use of social media. I accept that I will be held responsible where any images I may have shared with others (e.g. family members) are uploaded to social media.

Name & Signature of the parent: Santosh Daniel

### **Parent Consent Form**

Please complete and return: -

Child's name:	<u>Harigovind</u>
Class & Division :	8 C

Type of Consent	Yes	No
I give consent for the school to take digital images and videos of my child	Yes	
I give consent for the school to mention the name or any other required details of my child to be used on the official school web site or official Face book page.		No
I give consent for digital images of my child to be used on the official school web site.	Yes	
I give consent for digital images of my child to be used on the school's official Face book page.	Yes	
I give consent for digital images of my child to be used in the school prospectus and other promotional material for the school, such as flyers and leaflets.	Yes	
I give consent for digital images of my child to be used in internal displays.	Yes	
I give consent for digital images of my child to be taken when involved in school events; such as Assemblies, Sports Day etc. The school may make these recordings available to other parents.	Yes	

I hereby agree to the Schools terms and conditions especially regarding the use of social media. I accept that I will be held responsible where any images I may have shared with others (e.g. family members) are uploaded to social media.

Name & Signature of the parent:

Sreejith Achuthan Nair

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**



# **AL AMEER ENGLISH SCHOOL, AJMAN**

## **SCHOOL SOCIAL MEDIA POLICY 2022 - 2023**

## Overview

To ensure clarity of use and guidance for staff, pupils and all users, regarding the use of social media and networking applications. This policy is designed to protect individual members of staff, pupils and all users. This policy applies to the use of social media for both business and personal purposes, whether during School / working hours or otherwise. This policy applies regardless of whether the social media is accessed using school IT facilities and equipment or equipment belonging to members of staff, pupils or any other IT/internet enabled equipment.

## Scope:

The School defines social media as ‘any websites and applications that enable users to create and share content or to participate in social networking’. Social networking sites and tools include, Snap chat, Telegram, Netflix, Rowlocks, GROUPME, KIK Messenger, Discord, Tumblr, Text chat, Facebook, YouTube and Instagram.

## General policy Statements: -

Al Ameer uses a number of different methods to maintain effective communication with parents and guardians, other schools, the wider community and outside agencies. Depending on the nature of the communication, the school will use the most practicable means to contact the recipient. Communication on issues that affect the safety and wellbeing of a pupil will be treated as a priority. The school holds emergency contact details for all pupils, and families are asked to alert the school immediately if contact information needs to be revised. Staff will always seek to establish friendly relationships with parents and guardians but they will ensure relationships are professional and parents will be addressed in a formal manner. Staff are to avoid developing close relationships with parents and guardians. The use of a parent, guardian or staff member's first name is not appropriate, therefore all communications will be to and from Mr, Mrs, Miss, Ms, Dr etc.

The school has social media coordinator is Mrs. Riffat Tarique who can be contacted in times of crises or when need arises.

## **Roles & Responsibilities: -**

### **Key Roles of Social media coordinator:**

The school's social media coordinator makes sure that,

- The up-to-date updating of websites.
- Stakeholder's personal information's are not published in the school website.
- Website contents should have published only after Verified and approved by Principal.
- Signed Social Media Agreement form should collect from the parent before posting students images & activities on the website.
- Social media coordinator is responsible for the regular monitoring and filtering the improper content from the website with the permission of principal.
- Responsible for filtering and regularly monitoring all the school social media platforms.
- Inform the IT Admin to block the unwanted website from the school network.
- Viewing the website history and reporting the content access to OSL.
- Communicating the reported Incident with OSL.

### **Guidance and advice for staff:**

Most common social networking sites are inherently insecure places to have discussions which contain any sensitive information. Privacy laws can be violated and the reputation of our school can be damaged if the public sees a discussion of any sensitive information taking place on social network. Staff should be aware that these types of cases can result in disciplinary action.

Staff are not permitted to share information which is confidential and proprietary about the School. This includes information about services, programmes, financial, strategy, and any other internal confidential, proprietary, or sensitive workplace information that has not been publicly released by the School.

Staff must not discuss pupil or family related information via social networking and public social media, texting, or online unless it is an approved medium and for a school related purpose.

Staff must not publish photographs of pupils without the written consent of Social Media Policy – parents / carers, or the pupil themselves if they are deemed of the age and ability to provide their own consent. Standard practice is to publish only the first name and initial of surname, unless permission has been given by parents or pupils (if deemed of the age and ability to provide their own consent) for the full name to be used. School sanctioned social media sites must use images of children in suitable clothing.

**Use of social media in practice for pupils:**

- Pupils must not access any social media that is appropriate for adults only or if the pupil does not meet the minimum age requirement.
- Anonymous sites must not be accessed as there is a high risk that inappropriate comments can be exchanged, causing distress or endangerment.
- Bad, including offensive, explicit or abusive, language and inappropriate pictures must never be included in messages.
- All messages should be positive and not include anything that could be upsetting or defamatory towards others or the School.
- Pupils must take responsibility for keeping details of their accounts private, using full privacy settings and logging off properly and not allowing others to use their accounts.
- Pupils must report anything offensive or upsetting that they see online to the appropriate bodies, either by using the “report abuse” tabs or by speaking to their parents or a member of staff.
- It is a serious offence to use another person’s account, or to create an account in another person's name without their consent.

**Use of social media in practice for parents:**

- Positive contributions to the School Social Media, such as face book & YouTube are, welcomed.
- Any concerns or issues about the School, its pupils or staff should be expressed directly to the School and not be voiced on social media.
- Parents must obtain permission before posting pictures that contain other parents or their children, unless sharing or liking a post from the School's official social media account.
- If parents become aware of inappropriate use of social media by their own or other people’s children, they should contact the School so that

the School can work with the parents to educate young people on safe and appropriate behavior.

### **Media Consent Form**

Dear Parent / Guardian

During the school year, we take photographs of school activities involving students to share the school's positive vibe and updates. By which incidentally, some photographs may capture your child's participation, directly or indirectly. These photos may be published through our website, social media pages, news bulletins, billboards, and ads etc. So we request you to carefully read the points below.

I understand that:

- My child's photograph may be used within the school for display purposes.
- My child's image may be used in Learning Journeys or Records of Achievement belonging to other children.
- My child's image may be used on the school website, school newsletter, school social media accounts e.g. Facebook, Instagram etc.
- My child's photograph may be used in local and/or national media.
- My child may be filmed by the school during school events.

#### **Video Filming:**

During school events we accept that many parents may wish to film their child. However, all parents must agree to the following terms and conditions

- All filming is for personal use only and must not be shared with external agencies.
- No video, film or still photography from school events may be posted to any form of social media.

#### **Terms and Conditions:**

- This form is valid for the period your child attends this school. Images of your child will not be used after this time.
- Please write to the Principal if you wish to withdraw consent at anytime.
- The images we take will be of activities that show the school and children in a positive light.
- Embarrassing or distressing images will not be used. The images will not be associated with negative or sensitive issues. We will only use images of pupils who are suitably dressed.
- We will make every effort to ensure that we do not allow images to be taken of any children for whom we do not have permission or who are 'at risk'.

#### **Media Consent Form Agreement:**

I confirm that I have read and understood all school terms and conditions and that I agree to abide by their use.

Name of the Student: .....

Name of the Parent: .....

Signature: .....

Signature: .....

Date : .....

25

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**





# **AL AMEER ENGLISH SCHOOL, AJMAN**

## **SCHOOL PASSWORD SECURITY POLICY**

**2022 - 2023**

## Suggestions For Use:

Securing sensitive data is becoming more and more difficult with users having access to so many devices, Wi-Fi and internet connectivity. Single Sign on and shared accounts means a security leak on one system could allow unauthorized access to others. Teachers and pupils have access to data, documents and systems from home, the school network via Wi-Fi from the school grounds and with cloud email and storage a lost password could give malicious users easy access to a host of systems.

Staff and students often don't realize the potential risks this poses and it is important that e-Safety training and guidance helps to educate both groups of users.

Tablets, iPads, mobile phones, cameras and home laptops often don't support good practice with required passwords and it is important that schools also consider the types of data held on these devices, particularly if leaving the school.

Schools should provide a safe and secure username and password system. This policy template has been written to provide guidance on how schools may wish to develop their own policy.

## Introduction:

The school will be responsible for ensuring that the *school data and network* is as safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is applied to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE), School Orison portal as is reasonably possible and that:

- Users can only access systems and data to which they have right of access
- Users should agree to an acceptable use policy
- Users should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- Users must not store their passwords in plain view and staff must not write down passwords.
- Access to personal data is securely controlled in line with the school's personal data policy
- Where possible logs are maintained of access by users and of their actions while users of the system.

A safe and secure username / password system is essential if the above is to be established and will apply to all school IT systems, including email and Virtual Learning Environment (VLE).

## Implementation:

Staff and pupil accounts must be disabled on leaving the school and user data deleted after 3 Months. School office staff should ensure that the ICT helpdesk is aware of the leavers as soon as possible.

All users must change their passwords occasionally to ensure systems remain secure. However, the length between changes needs to take into account the type of user and the risk to the school if unauthorized access was gained. Similarly the complexity of password needs to reflect the user.

### ***Users should change passwords to the following schedule and complexity***

- Staff password every 90 days : Minimum 8 characters  
(Access only for the Staff)
- Grade KG1 to Grade 5th every 60 days : Minimum 8 characters  
(Access only for the Parents)
- Grade 8th to Grade 12th pupil every 60 days : Minimum 8 characters  
(Access to Parents or Students)
- Foundation pupils class account every 365 days

## Instruction for creating the password

1. Should contain 8 characters
2. Should contain alpha numeric characters
3. Should include special character (e.g., ~, !, @, #, \$, ^, (, ), \_, +, =, -, ?, )
4. Contain at least one number (e.g., 0-9)
5. Should contain upper- & lower-case characters (Aa – Zz)
6. Should not include personal data
7. Should not repeat any characters more than twice
8. Should not contain a dictionary word in any language, slang, dialect, jargon, etc

Tablets or other devices syncing to email, cloud storage or storing data not able to meet these requirements must as a minimum use 4-digit pin codes with a lifespan of 60 days for staff or 365 days for pupils. The mail administrator may enforce stricter requirements.

### Policy Statements:

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).

All users (KG and above) will be provided with a username and password. Users will be required to change their password at set intervals. Class log-on for foundation pupils may be used but the school needs to be aware of the risks associated with not being able to identify any individual who may have infringed the rules set out in the policy. Use by pupils in this way should always be supervised and members of staff should never use a class log on for their own network access.

The following rules apply to the use of passwords:

- *The account should be “locked out” following six successive incorrect log-on attempts*
- *Temporary passwords e.g. Used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log-on*
- *Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *Requests for password reset for a pupil should be requested by a member of staff. Password reset for a staff accounts must be requested by the individual directly.*

Where sensitive data is in use – particularly when accessed on laptops – schools may wish to use more secure forms of authentication e.g. two factor authentication such as the use of hardware tokens and if so should add a relevant section in the policy. Where this is adopted, the policy should state clearly that such items as hardware tokens must be stored separately from the laptop when in transit – to avoid both being lost / stolen together.

### Roles & Responsibilities

All users provided with their own user accounts will have responsibility for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately change their password and report any suspicion or evidence that there has been a breach of security. Class accounts used for foundation pupils should be monitored by the class teacher and pupils should only use under supervision.

*New user accounts, and passwords for existing users will be allocated by the IT Incharge.*

**Class Teacher**

1. CT will receive information from class students, when their school login Id is not working.
2. CT will share the student information to the OSL and Head teacher.
3. CT will receive the New Password from the IT Coordinator and share to the student.

**IT Admin**

1. IT Admin will receive the official information from the OSL when a student can't login into the account.
2. It will be informed to the concerned IT coordinator.
3. Daily report of password resetting will be given to the OSL.

**Supervisor**

1. Supervisor will receive the information about student's login problem from the class teacher.
2. Supervisor will inform the same to the section IT coordinator officially.
3. Supervisor will have a supervision over the problem resolving in their sections.

**IT Coordinator**

1. IT coordinator will receive the student's login issue for the CT and conformation from the section Supervisor.
2. IT coordinator will solve the login issues and share the new password to the Class teacher.
3. Daily report will be send to the IT Admin about their section login issues.

**OSL**

1. OSL have the overall communication with the SLT member.
2. As per the request get from the C.T will check and confirm with Supervisor
3. Whether it is relevant case inform to the IT Admin for password reset.
4. Giving proper training to the team.
5. Maintain the password reset Log from IT Admin.

**Principal**

1. The person who have the overall controlling of the entire system.
2. Observing and verifying the duties and responsibilities of all the In charges.
3. Taking proper action against the incidents.
4. Communicating and dealing with the external vendors for outside help.

**Audit / Monitoring / Reporting / Review :**

The Password Security in charge will ensure that full records are kept of:

- *User Ids and enabled accounts*
- *Security incidents related to this policy*
- *Password Changes and Complaints*

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

(In Maintained schools) Local Authority Auditors also have the right of access to passwords for audit investigation purposes

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by ... (*E-Safety Officer / E-Safety Committee / E-Safety Head*) at regular intervals *annually*.

This policy will be regularly reviewed annually in response to changes in guidance and security incidents.

### **Training / Awareness:**

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorized access / data loss. This should apply to even the youngest of users, even if class logons are being used.

Members of staff will be made aware of the school's password policy: □ at introduction

- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement Policy

Students will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place) through the Acceptable Use Agreement

### **Evaluation :**

This policy will be reviewed as part of the school's review cycle or if guidelines change

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL FILTERING POLICY**

**2022 - 2023**

## Overview

The main reason that Al Ameer English school implement filtering controls may be **to prevent students from accessing age-inappropriate website content**, but the extent to which cybercriminals are conducting cyberattacks on schools, blocking the malware that gives them access to school networks is vital. Keeping students safe from the internet is paramount in our school safeguarding policies, with legislation requiring schools to have an appropriate filtering and monitoring service.

## Scope

*Finding the balance between over-blocking and protecting students from harmful content can be difficult.* Content filtering is a filtering system that can find the balance between blocking and not reducing learning resources. We will look at what content filtering is, how much control you have with the system and why content filtering is essential for education and safeguarding.

This policy applies to all communications between the school's networks and the Internet, including web browsing, instant messaging, file transfer, file sharing, digital content, social media content school website content. This policy covers all stakeholders of our school.

## General policy Statements: -

Al Ameer English School ensures the following points in our Policies:

1. The school maintains and supports the managed filtering service provided by the Internet Service Provider.
2. The school/academy manages its own filtering service
3. The school has provided enhanced/differentiated user-level filtering through the use of the filtering programs.
4. In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head teacher/Principal (or other nominated senior leader).

5. Mobile devices that access the school/academy internet connection (whether school/academy or personal devices) will be subject to the same filtering standards as other devices on the school systems.
6. Any filtering issues should be reported immediately to the filtering provider.
7. Requests from staff for sites to be removed from the filtered list will be considered by the technical staff. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the Online Safety Group.

The methods of filtering applied in different school systems.

### **A. Google Class Room (VLE) FILTERING**

The GC under “Al Ameer School” domain ensure that,

- 1) GC ensure the safe and secure learning for the Students.
- 2) Authorized members are permitted to join the class rooms.
- 3) The digital learning materials uploaded in GC for students are proofread by the concern subject teacher and approved by HOD to make sure that it is relevant and age appropriate.
- 4) HODs & Supervisors monitor the classes consequently as per schedule.
- 5) IT Admin have the overall control and monitoring of the system, if any improper activity occurs he can filter/block the user.

### **B. School Website & Social Media Filtering**

The school’s social media coordinator makes sure that,

- 1) The up-to-date updating of websites.
- 2) Stakeholder’s personal information’s are not published in the school website.
- 3) Website contents should have published only after Verified and approved by Principal.
- 4) Signed Social Media Agreement form should collect from the parent before posting students images & activities on the website.
- 5) Social media coordinator is responsible for the regular monitoring and filtering the improper content from the website with the permission of principal.

### **C. School device**

- 1) Differentiated filtering is implemented inside the network to access different stakeholders using firewall (Fortinet 100F BDL Firewall).
- 2) School systems will be provided to staffs and students with updated Antivirus protection.

- 3) Two user account/ login system (Admin & user) were setup in all the school devices, Admin account have overall controlling of the system.
- 4) School's computer Lab systems are configured using 'N' Computing technology.

## **Roles & Responsibility of Stakeholders: -**

### **Social Media Coordinator**

1. Responsible for filtering and regularly monitoring all the school social media platforms.
2. Inform the IT Admin to block the unwanted website from the school network.
3. Viewing the website history and reporting the content access to OSL.
4. Communicating the reported Incident with OSL.

### **IT Admin**

1. Maintaining the list of blocked website in school network.
2. Unblocking the website as per the request from the SMC.
3. Monitor all the school system consequently and update the software as per user's requirement.
4. Remind Principal regarding the license renewal of firewall, antivirus, School software's etc.

### **OSL**

1. Regularly observing all the school system were filtered from inappropriate content.
2. Instruct and provide the list of blocking website to the IT Admin.
3. Maintaining the Incident reports.
4. Communicating the Incident reports with SLT.

### **Principal**

1. The person who have the overall controlling of the entire system.
2. Observing and verifying the duties and responsibilities of all the In charges.
3. Taking proper decision and action against the incidents.
4. Communicating and dealing with the external technical network experts help.

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL TECHNICAL SECURITY POLICY**

**2022 - 2023**

## Overview

The term 'technical security' refers to the techniques used for authentication and protection against theft of proprietary information and intellectual property, which are both increasingly at risk of industrial espionage.

The Al Ameer English School Ajman has an effective technical security strategy that ensure the technical security of all the school system such as Google class room, School Orison software and all school devices connected with network.

## Scope

This Policy is applicable to staff, students, parents, external parties and to all users of Al Ameer English School, whether they are officially affiliated with our School or not, and whether on campus or from remote locations.

This Policy applies to all devices, both School-owned computers (including those purchased with grant funds) and personally-owned computers that connect to the Al Ameer School network and store the information. The contracts and agreements shall include statements whereby all the stakeholders agree to comply with this Policy.

## Policy Statements

Al Ameer English School is committed towards securing the confidentiality, integrity and availability of information for the education purposes. The security of information is therefore regarded as vital for the successful education of us.

The following security mechanism were applied for providing the security.

### A. Firewall Policy

#### **Device: Fort iGATE 100F BDL Firewall Configuration**

Firewall provides a wide range of security and connectivity features, including web filtering, website monitoring etc. Content filtering is the use of a program to screen and exclude access to web page or email deemed objectionable

#### **Service Provided**

- 1) Content filtering and web monitoring to prevent students from accessing inappropriate materials online, to alter school leaders to cyber bullying and other instances in which student's digital communications or web activity might indicate troubling behavior.
- 2 Firewall protection to defense and stop a malicious program or attacker from gaining access to the school network and information before any potential damage is done.

This Agreement is created to establish the SCHOOL WEBSITE MONITORING, FIREWALL PROTECTION AND CONTENT FILTERING SERVICES, including maintenance and management services that the Service Provider shall provide to the client in relation to the agreement agreed by the parties. With this Agreement, the Parties understand the mutually agreed Services that shall be performed and the accompanying exceptions of the parties.

## **PERFORMANCE INDICATORS**

The Service Provider shall maintain the records and reports of the service levels reached and exceeded in the given month. The representatives, appointed respectively by the Parties, shall assess the performance of the Service Provider to ensure that the all level targets are maintained.

## **B. System Security**

**Server > HP 380DI Intel Xenon 2.20GHz**

**Operating System > Windows Server 2012 R2**

1. All Desktop and laptops are under the domain.
3. All devices are using individual static IP and are connected with domain
4. Staffs, Teachers and students are provided user id and passwords for access under the domain
6. Data backups are accessed every day by IT Admin
8. Access to server is only given to IT Admin.

## **N- Computing**

**Operating System > Windows Server 2016 SNGL Academic Core**

1. Students Computer Lab are connected with N-Computing technology
2. The students work will be automatically updated in the server systems.
3. All the systems are controlled by the Server.
4. All software updation is doing in the server will reflects the client systems.

## **Antivirus**

**Software> Kaspersky**

The features of Kaspersky Anti-Virus used in Al Ameer English School include real-time protection, detection and removal of viruses, trojans, worms, spyware, adware, keyloggers, malicious tools and auto-dialers, as well as detection and removal of rootkits.

1. All school devices or networked resources shall have anti-virus software installed, configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices.
2. All files on computer devices will be scanned weekly for viruses.
3. An infected computer device may be disconnected from the network until the infection has been removed.
4. Antivirus expiry date should be informed prior to IT admin
5. Websites are preventing from virus.

## **C. VLE Security**

### **Platform> Google Meet**

1. It is registered with our school domain to restrict the usage of public.
2. All user's ID's shall be provided under the school domain name.
4. All accounts are managed and monitored by IT admin
5. It is compulsory for all users in this domain to change the password once in every 60 days.
6. Students are restricted to create meetings, individual group and personal chat among themselves.

## **Roles & Responsibility of Stakeholders**

### **Principal and Senior Leaders:**

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Principal and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles

## **Online Safety Leader:**

- Leads the E-safety Team.
- Takes day by day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the IT Admin to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

## **IT Admin:**

- The IT Admin is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements and any SPEA / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Year / Principal / Senior Leader; E-Safety Coordinator

## **External Communication details**

*Emergency contact number:-999*

*Toll free number:8002626*

*Email:mail@dubaipolice.ae*

## **Firewall Implementation**

*Tel: 0561716669/ 0547596669*

*E-mail : [info@cascadeworld.net](mailto:info@cascadeworld.net)*

## **Hira Computer Solution**

*Tel: 065234925*

*E-mail : [mail@hirasolutions.com](mailto:mail@hirasolutions.com)*

**Policies Implementation:** MARCH 2020

**First Review Date:** JANUARY 2021

**Second Review Date:** APRIL 2022

**Next Review Date:** JANUARY 2023



# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL DATA PROTECTION POLICY  
2022 - 2023**

## Overview

The COVID-19 pandemic has brought unprecedented challenges to our safety, health and education. In the process of online learning, Personal data are produced through the interaction between students/teachers and tools or platforms. Personal data and privacy are the tranquility of the private life of a natural person, and the private space, private activities, and private information that one is unwilling to be known to others

Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights, also known as Wadeema's Law (PDF, 250 KB), states: The telecommunications companies and internet service providers shall notify the competent authorities or the concerned entities of any child pornography materials being circulated through the social media sites and on the Internet and shall provide necessary information and data on the persons, entities or sites that circulate such material or intend to mislead the children.

In addition, the Dubai Data Law (Law No. 26 of 2015 on the Organization of Dubai Data Publication and Sharing, PDF 250 KB) aims for data protection and privacy of all individuals including that of children.

## Scope

### CYBER SECURITY POLICY

Top cyber security threats for schools includes:

- Phishing - The practice of sending legitimate-seeming emails that will entice users to reveal personal information or click on links that install malicious software.
- DDoS - A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of the district servers.
- Data breach - A data breach is the release of secure confidential information
- Ransomware - A type of malicious software that encrypts the district's data and requires a ransom to be paid in order to regain access to the data.

Cyber security policy exists to ensure that all staff, students and third parties follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff coming to harm as a result of others accessing intolerant, extremist or hateful web sites.

The school ensures,

1. Cyber security for all student and staff.
2. Critical use of technology delivered to the appropriate user groups.
3. Users understand their IT security.
4. A culture of security awareness and persistent maintenance program to ensure continual awareness is built.
5. Responsible, safe and intelligent use of Information Technology.

6. Sensitive information is protected from unauthorized disclosure.
7. Integrity is maintained through accuracy, completeness, consistence and timeliness of data.
8. Safeguarding necessary resources and associated capability.
9. Cyber bullying is totally curbed.
10. Investigation into incidents of cyber bullying.
11. Parental and peer support for cyber safety.

## **PROCEDURE:**

1. Dent in confidentiality of records will result in suspension or dismissal/ termination for a term /year/permanently.
2. Improper use or display of information technology in school will initiate serious disciplinary action.
3. Backup data on a server that is not accessible by the rest of the network and therefore not vulnerable to the ransomware encryption agent.
4. Train end users in what data they are responsible for protecting and how to handle data.
5. Training staff to detect and report suspicious e-mails is the first and most important step to deal with phishing.
6. Cyber bullying will be dealt with severe disciplinary actions.

## **DATA SECURITY**

The data within the school's systems and networks may be the most valuable asset. In establishing the physical security measures and user access framework, the school should also pay attention to the protection of data. In general, data security requires data files to be properly created, labeled, stored and backed up. The data should also be protected from attack.

Some of the common IT security controls for data protection we follow include:

- Physical Security
- Access Control
- Password Management
- Data Security
- Network and Communication Security
- Data backup & Recovery
- Security Audit and Incident Handling
- User Awareness and Education

## **PHYSICAL SECURITY:**

The IT equipment, such as servers, workstations, backups, recovery diskettes, original software packages etc. are kept in a safe place against unauthorized access.

## **ACCESS CONTROL:**

Access controls are defined for and assigned to specific data files, resources and other system rights. Role based access control is followed as users are allowed to access only specific information

## **PASSWORD MANAGEMENT:**

Password complexity, minimum and maximum length is set for e learning platforms. Parameters like number of invalid password attempts, lockout duration and unlocking procedures are also defined

## **WIRELESS NETWORK SECURITY:**

The School endeavor to have all access points located in physically secure locations, and access to wireless management is limited and have strong authentication.

To prevent unauthorized access faculty, staff and students must use strong passwords. All default passwords are changed. On occasion, when guest access is required, the guest network is enabled and the password is given out. The guest password is changed regularly. Passwords are regularly changed to ensure access is gained only by authorized users.

The access to wireless management is limited to the Systems Administrator or the designate, using an account with a strong password

Automatic updates are configured to keep access point software patched.

Routine Checks - The network administrator checks for rogue devices monthly, and unidentified devices are denied access.

Firewall Rules and Application Rules - wireless access point, firewall rules and application rules, as well as an encrypted password for the SSID are configured to help prevent and minimize virus and malware programs from being installed, or gaining access to sensitive, confidential or financial data.

## **NETWORK AND COMMUNICATION SECURITY:**

Users accessing to school online platforms and network are properly administered and monitored.

## **BACKUPS AND RECOVERY:**

All backup and recovery procedures are well documented, tested and properly implemented. System administrator is responsible for data backup and recovery. Data backup should be performed and monitored at regular intervals. Periodically, it is advised to perform a trial restoration to verify that files could be properly backed up

## **SECURITY AUDIT AND INCIDENT HANDLING:**

Security logging is followed to detect the occurrence of threats. Monitoring and review of the school's online platform and networks on a periodic basis for IT security incidents

## **USER AWARENESS AND EDUCATION:**

School provides well-conceived and committed security training programs, which enable users to be better prepared to avoid incidents.

### **Policy Statements**

- 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
- All personal data records held by the school are obtained, processed, used and retained in accordance with rules of data protection.
- Appropriate access privileges of the different data classes are assigned to different users according to their needs
- Users under school domain can only access our e learning platforms.
- Public data intended for all users are published in school website, for example, school announcement.
- All end users of e learning plat forms should install and configure anti-virus software in order to protect data.
- Parents can report any complaints related to data protection to class teachers and class teachers must notify Top Admin

- Data backup should be performed and monitored at regular intervals. Periodically, it is advised to perform a trial restoration to verify that files could be properly backed up
- Data communications are encrypted and password protection feature is available in school application software for protecting documents containing sensitive data
- The School shall process personal data of children and staff in a manner that protects and advances the rights and best interests of the individual.
- The virus monitoring and real time alert functions should be activated in all servers and workstations
- For security incident handling a team is assigned including teachers, supervisors, top admin and IT personals.

With Warm Regards

A handwritten signature in black ink, appearing to read 'S. J. Jacob', with a stylized flourish at the end.

S. J. Jacob  
Principal

## **AUDIT OF SENSITIVE DATA**

Classrooms have become increasingly networked environments that may put the privacy of children at risk. Specifically, these connected classrooms raise issues of transparency, in view of the fact that inappropriate data processing practices by e-learning platforms, opaque automated decision-making and misuse of learning analytics risk undermining data protection and privacy rights. In the case of children and youth, this can have significant and long-term social, economic and professional consequences, and fail to account for their evolving capacities. We are doing the following steps to ensure the sensitive data protection.

- Teachers are equipped with up-to-date, relevant and sufficient information on data protection and privacy
- Developed policies and procedures to evaluate, approve and support the use of e- learning platforms and, where feasible or required, conducts data protection/privacy impact assessments.
- Where required or appropriate, seeks valid, informed and meaningful consent from individuals.
- We ensure that e-learning platforms appropriately safeguard users' personal data and meet the appropriate data protection standards (SSL certified)
- All collection of student data is limited to what is needed for educational purposes.
- Administrative, physical and technical safeguards are in place to ensure the lawful processing of all personal data in compliance with applicable requirements and avoid the risk of inadequate security
- Continuously monitor and improve technological and organizational measures for data security.

### **PROCEDURE:**

- School management conducts periodic audits of data protection.
- A cyber security committee is appointed to oversee responsibility for data protection.
- Cyber security committee evaluates current practices and procedures to ensure that they meet the demands of the Data Protection Acts and identify, analyze, and correct hazards to prevent a future re-occurrence.

## **DATA LEVEL OF ACCESS**

- **Staff Data** – All Staff Data can be accessed by HR. Receptionist can access minimal details like phone number for communication purpose

- **Student Data** –

Admission Officer – Ms. Selma Mohammed Kutty - has the complete access of Student data

- **Data Base Access-**

Data base can be accessed by IT Admin – Mr. Navas Rahimkutty, Ms. Fathima, Ms. Shafna

# LEVELS OF DATA BASE ACCESS AUTHENTICATION

- Password-based authentication –

All users of the school software and portal has username and password

- Multi-factor authentication-

Multifactor authentication (MFA) for Gmail accounts

## **External Communication details**

*Emergency contact number:-999*

*Toll free number:8002626*

*Email:mail@dubaipolice.ae*

## **Firewall Implementation**

*Tel: 0561716669/ 0547596669*

*E-mail : [info@cascadeworld.net](mailto:info@cascadeworld.net)*

## **Hira Computer Solution**

*Tel: 065234925*

*E-mail : [mail@hirasolutions.com](mailto:mail@hirasolutions.com)*

**Policies Implementation: MARCH 2020**

**First Review Date: JANUARY 2021**

**Second Review Date: APRIL 2022**

**Next Review Date: JANUARY 2023**



Tel: 06 5234925  
Mobile: 050 3099500  
PB No: 62054  
Sharjah, UAE  
E-mail: mail@hirasolutions.com  
www.hirasolutions.com

Customized Software Solutions for Accounts, Inventory, Production, Costing, HR, Real Estate, Schools & Colleges

### Agreement

This is the Support Renewal of agreement signed between Al Ameer English School, Ajman and Hira Computer Solutions, Sharjah regarding the Maintenance of Orison School Management system, Academic portal and Mobile APP. This Agreement contains the following.

#### Orison School Applications

The Software will be maintained in the school server which uses SQL Server Database and Microsoft .Net technologies.

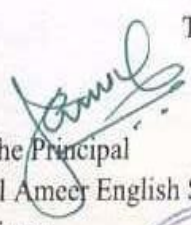
#### AMC Module Details:

Orison School ERP Modules  
Mark and Grading Module  
Parent portal and Mobile APP  
Website Hosting  
Google Gsuite Support

#### Annual maintenance

The maintenance contract is for 1 year valid from Apr-2020 to Mar-2021

This agreement signed on APR 2020

  
The Principal  
Al Ameer English School  
Ajman



  
The Manager  
Hira Computer Solutions  
Sharjah





# **AL AMEER ENGLISH SCHOOL, AJMAN**

**SCHOOL INDUCTION POLICY  
2022 - 2023**

## INTRODUCTION

Al-Ameer English School is committed to safeguarding and promoting the welfare of the children in its care. The induction programme is a vital process that is undertaken to support newly appointed staff, volunteers and students. An effective induction programme for teachers and support staff is essential to maintain continuity of purpose and benefit from the additional expertise the new member of staff will bring.

## AIMS

Our priority is to raise standards and improve the quality of e- learning for all our pupils in a safe and attractive welcoming environment. The Induction Policy and the Induction Procedures aim to provide all newly appointed staff, and those changing role, with a program of structured e-learning support and guidance appropriate to their role.

## POLICIES TO STUDENTS AND PARENTS

1. Introduction of schools' policies and practices to students, teachers and parents
2. Use of school portals and credentials
3. The school's Code of Conduct– making clear the expected standards of conduct and behavior
4. The school's policies and procedures, including safeguarding, acceptable use of ICT
5. Requirements for reporting absence
6. Health and Safety procedures explained and training received if necessary
7. Advised on how to report any issues in online classes
8. School timing and punctuality policy
9. Absenteeism policy
10. Personal standards/ behavior, code of conduct or agreement
11. Dress code and standards of appearance
12. Student responsibilities
13. Students goals and targets

## **POLICIES TO TEACHERS**

1. Introduction of schools' policies and strategies
2. Introduce the school website and its authenticity
3. Use of school portals and credentials
4. The school's Code of Conduct– making clear the expected standards of conduct and behavior.
5. The school's policies and procedures, including safeguarding, acceptable use of ICT
6. Requirements for reporting absence
7. Health and Safety procedures explained and training received if necessary
8. Advised on how to report any issues in online classes
9. Work timing and punctuality policy
10. Absenteeism policy
11. Personal standards/ behavior, code of conduct or agreement
12. Dress code and standards of appearance
13. Student responsibilities
14. Students goals and targets
15. The New National Curriculum
16. Staff values (school vision)
17. School Prospectus
18. Access to Policy documents
19. Assessment advice, recording, reporting, resources and procedures
20. Class list
21. Child Protection
22. Safeguarding
23. Behavioral Policy
24. Information on whole school and year group resources, including ICT

25. E-Safety
26. Timetables
27. SEN information
28. Roles and Responsibilities of all staff
29. Educational Visits Policy

## **Regular evaluation and review**

The teaching and learning in our school will be a dynamic process with both students and teachers as strong partners. The students in our class-rooms would know

1. How to make progress;
  2. What they are achieving through self-assessments;
  3. How to learn, including thinking and questioning skills, using methods and resources;
  4. The challenges and support available to them;
  5. The attitudes needed in the classroom, including respect, interest, responsibility, responding to challenge
  6. how to work collaboratively
  7. The skills they need to develop, including enquiry, research, analysis, reflection.
- Students will be provided a basic frame – work of expectations and guidelines. Teaching through not just directions but activities-based methodology and utilization of educational resources is an important tool to engage student's classrooms. The range of teaching and learning styles used at our School will be extensive. These will include: Explanation, Instruction, Questioning, Observation, Modelling, Investigation, Problem solving, Individual work, Collaborative work, Using ICT, Extended writing, Songs / rhymes, Discussion, Demonstration, Listening, Oral Feedback. During the lesson planning, all aspects of learning is considered which aligns with the objective of the lesson, procedures and activity, assessment, use of resources.

**Policies Implementation:** MARCH 2020

**First Review Date:** JANUARY 2021

**Second Review Date:** APRIL 2022

**Next Review Date:** JANUARY 2023