الإمـــارات
The Emirates

We track Your Child's Future
al ameer
English School

نعمل لمستقبل أولادكم
الأمـــيــر
مدرسة الإنجليزية

E-SAFETY POLICY 2020-21

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, Behaviour, 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 / carers, 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 behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. 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 behaviour and anti- bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behaviour that take place out of school.

MONITORING / REVIEW OF DOCUMENTS – 2020-21

SCHEDULE FOR DEVELOPMENT / MONITORING / REVIEW

This E-safety policy was approved by the Governing Body on:	5 April'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 demand)
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 / Carers
  - Staff

Roles and Responsibilities:

E-SAFETY TEAM

Mr. S.J. Jacob	-	Principal
Mr. Nowshad Shamsudeen	-	Vice Principal (E-safety Governor)
Mr. Saifudheen P Hamsa	-	Academic Coordinator
Mrs. Latha Anilkumar	-	Curriculum Head
Mrs. Ahlam Mustafa	-	Arabic Secretary
Mrs. Haseena Riza	-	E-safety Coordinator
Mrs. Jotsana Sasi	-	IT Coordinator
Mr. Navaz Khan	-	IT Staff
Mrs. Fathima	-	IT Staff
Mrs. Seema Joy	-	Office Staff
Mrs. Salma	-	Office Staff
Mrs. Geetha Rengasamy	-	Supervisor (Sec&Hr Sec-Girls)
Mrs. Shermila Unnikrishnan	-	Supervisor (Sec&Hr Sec-Boys)
Mrs. Sujatha Prakash	-	Supervisor (Upper Primary&Middle School – Girls)
Mrs. Riffat Mustaq	-	Supervisor (Upper Primary&Middle School – Boys)
Mrs. Beena Hamza	-	Supervisor (Lower Primary)
Mrs. Shaher Banu	-	Supervisor (Kindergarten)
Mrs. Sheena Mary	-	Teacher
Mrs. Zeenath Khan	-	Teacher
Mrs. Shazia Khan	-	Teacher
Shahan Cheralody	-	School Head Boy (Student E-Monitor)
Kadeeja Huda	-	School Head Girl (Student E-Monitor)

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 to 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 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 Co-ordinator / 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 / carers 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 copyright 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 their 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.

Parents / Caregivers:

Parents / Carers 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 & RESPONSIBILIES OF PARENTS DURING GLOBAL PANDEMIC

(For 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:
• Some may initially be happy to be home, but over time the disruption to their routine, isolation from friends, and other imposed limitations will increase their stress.
• Children may experience ups and downs in their behaviours 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 th 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 programme 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 carers 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 behaviours. 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 programme 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 programme, 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 organisations
- 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 organisation
- 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 up to 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 workstations 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. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated

- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

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, parents / caregivers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues 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 in 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 / carers 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 carers 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 carers

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 must ensure 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 and understood 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 must ensure 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 professional in 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 or KHDA
- 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

	Staff & other adults				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowe d	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					❖
	Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					❖
	pornography				❖	
	Promotion of any kind of discrimination				❖	
	Promotion of racial or religious hatred				❖	
	Threatening behaviour, including promotion of physical violence or mental harm				❖	
	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				❖	
Using school systems to run a private business					❖	
Use systems, applications, websites or other mechanisms that bypass the filtering.					❖	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					❖	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					❖	
Creating or propagating computer viruses or other harmful files					❖	
On-line gaming (non-educational)					❖	
File sharing					❖	
Use of social networking sites			❖			
Use of video broadcasting e.g. YouTube			❖			

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 the 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’ behaviour
    - ➢ 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 a 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 proportionate manner, and that members of the school community are aware that incidents have been dealt with.

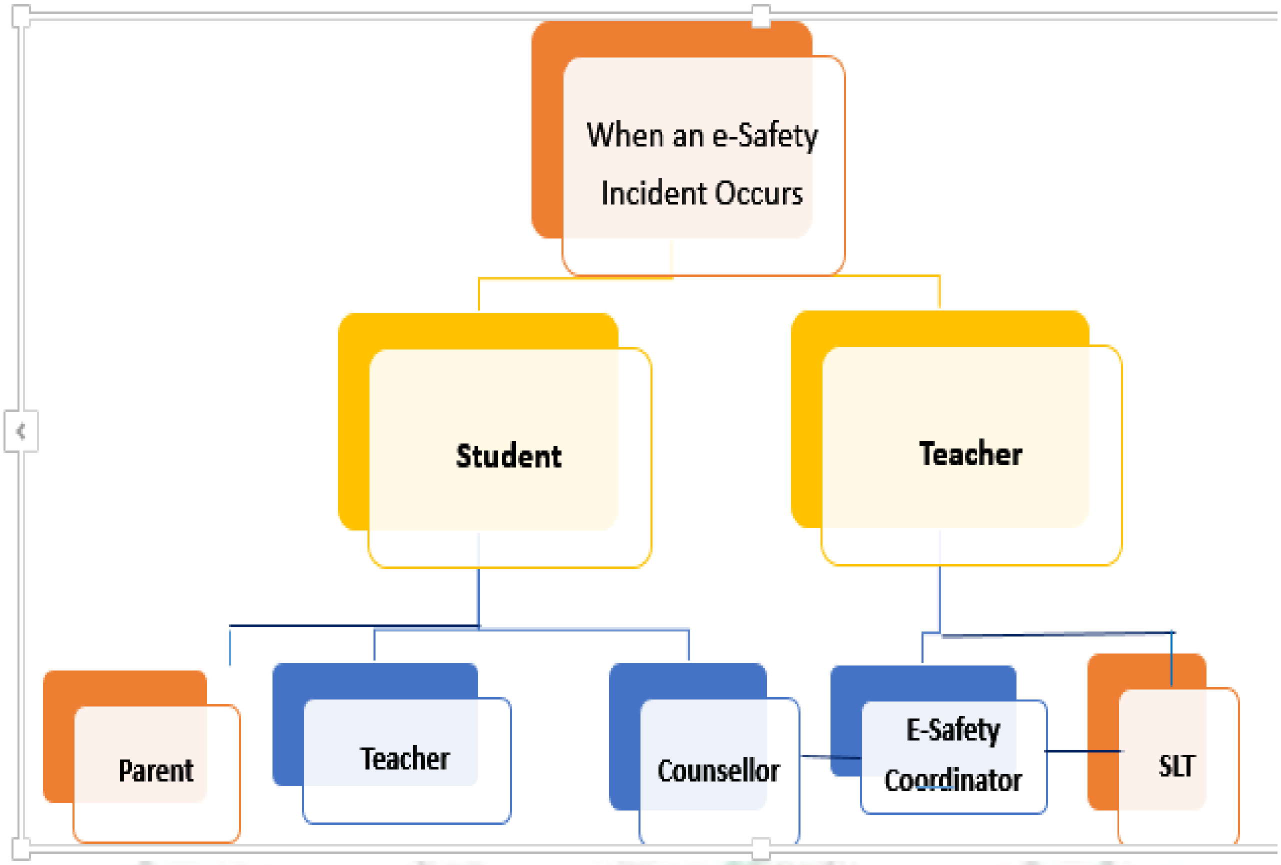
Actions (Students)

Incidents	Refer to class teacher	Refer to Co-ordinators	Refer to Principal / Vice Principal	Refer to technical support staff for action re filtering / security etc.	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).	❖		❖		❖	❖	❖		
Unauthorised use of non- educational sites during lessons	❖					❖	❖		
Unauthorised use of mobile phone / digital camera / other handheld device	❖		❖		❖				
Unauthorised use of social networking / instant messaging / personal email	❖					❖	❖		
Unauthorised downloading or uploading of files	❖				❖	❖	❖		
Allowing others to access school network by sharing username and passwords	❖				❖	❖	❖		
Attempting to access or accessing the school network, using another student's account	❖					❖	❖		
Attempting to access or accessing the school network, using the account of a member of staff	❖		❖		❖				

Actions (Staff)

Incidents	Refer to Principal / Vice principal	Refer to Directors	Refer to technical support staff for action re filtering / security etc.	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).	❖	❖					❖
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	❖			❖		❖	
Unauthorised downloading or uploading of files	❖			❖			
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				❖			
Careless use of personal data eg holding or transferring data in an insecure manner	❖			❖			
Deliberate actions to breach data protection or network security rules	❖			❖		❖	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	❖	❖			❖	❖	❖
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	❖	❖				❖	❖
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	❖			❖		❖	❖
Actions which could compromise the staff member's professional standing	❖			❖		❖	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	❖	❖				❖	

E-safety Reporting Flow Chart



Appendices:

1) Student & Parent Consent Form

2) Teachers & Staff Consent Form

3) Media Consent Form

Appendix-1:

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 inschool.
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 toschool.

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 atrisk.

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 aswell.

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:

- 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.

- 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.

- Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they have a week.

- 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.

- 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.

- 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.

- 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, clean up.

- 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.

- 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 :______________________

- 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.

Staff Online Acceptable Use Agreement

Name of the Employee: …………………….

Employee's Signature: …………………… Date: ………………………….

Appendix-3:

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 any time.
- 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 :*______________________**