11. CYBER SAFETY AND ETIQUETTE POLICY

10.1 Roles and Responsibilities:

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

10.1.1 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.

10.1.2 The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Coordinator
- 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.

10.1.3 Roles of 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 ADEK / 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 Network Manager / Technical staff.

10.1.4 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 / 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 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.

10.1.5. 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 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 Designated.

10.1.6. 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.

10.1.7 Cyber-bullying Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy.
- 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 Parents / Caregivers: Parents / Caregivers 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.

- 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) Community Users Community Users who access school systems / website as part of the wider school provision will be expected.

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 school's e- safety provision. 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 / PHSE / 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 evenings / sessions
- High profile events / campaigns
  - 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 UAE's federal Law, Article 378.

It 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 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

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.
- 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 Social Media. Protecting Professional Identity All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or ADEK liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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 ADEK.
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information; the school's / academy'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.

School Actions & Sanctions 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.