School of Knowledge

(St. Mary's Group of Schools)

E-SAFETY POLICY

TABLE OF CONTENT:

1. INTRODUCTION:

The E-Safety policy of School of Knowledge is developed to build resilience in students, to empower the staff and to involve and inform the parents to create an e-safe environment.

The purpose of this policy is to:

- Safeguard and protect the children and staff of the school.
- Set out the key principles expected of all members of the school community with respect to the use of technologies.
- Ensure that all members of the school community are aware of the guidelines on acceptable use of technology and the disciplinary or legal actions will be taken if unacceptable use is reported.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.

This policy will be reviewed periodically in consideration with the input given by parents, students and staff throughout the year according to surveys conducted by the school.

2. POLICY AND LEADERSHIP:

2.1. E-SAFETY TEAM

The E-Safety team is nominated by the SLT and positions are elected as per eSafe School Framework.

Role	Name
Principal/Vice Principal of the School	Mr. Peter Rowlands / Sr. Sarala
E-Safety Officer	Ms. Safeera
IT Administrator	Mr. Aris Del Rosario
E-Safety Committee	Ms. Ulfath Aslam (FS2 - Year 1) Ms. Bridget Shakesy Year 2-Year 4) Ms. Binu Paul (Year 5- Year 8) (Administrative Coordinators) Sr. Sarala (VP/Head of Pastoral Care/Well Being Team) Ms. Ambily Ms. Athelene Ms. Orlina Ms. Parul Ms. Lubna Ms. Safa Ms. Rivora (Counselor) Ms. Divyashree Ms. Mizbha Ms. Thasni, Ms. Dahlia (Arabic Translator)

2.2. ROLES and RESPONSIBILITIES

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school:

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 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 Officer 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.
- The principal will ensure that E-Safety is embedded within the wider safeguarding framework and is regularly reviewed as part of school development planning.
- The principal will Approve and review E-Safety policies and procedures annually or in response to significant incidents or changes in legislation.
- The principal will Promote a culture of responsible online behavior throughout the school.

E-Safety Officer:

- Leads the E-Safety committee.
- Takes day-to-day responsibility for E-Safety issues.
- 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 MOE / relevant body.
- Liaises with school technical staff.
- Maintains and updates the E-Safety policy in line with technological advancements and regulatory changes.
- Conducts regular E-Safety audits to identify and address areas for improvement.
- Coordinates awareness campaigns and workshops for students and parents on E-Safety best practices and digital citizenship.
- Maintains an incident log and reports patterns or recurring issues to senior leaders.

IT-Administrator:

IT-Administrator are responsible to manage all the IT network and system approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the school leaders, receiving regular information about E-Safety incidents and monitoring reports.

- Regular meetings with the E-Safety Officer.
- Regular monitoring of content filtering and firewall updates.

Software and System Updates

- Ensure all software, antivirus, and operating systems are kept up to date with the latest security patches and updates.
- 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 MOE / other relevant body guidance that may apply.

Access Control and Permissions Management

- Manage user roles and permissions to ensure users have appropriate access levels based on their roles within the school.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed and monitored.
- The content filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- 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 Principal/Senior Leader/E-Safety Officer.

E-Safety Committee:

- Promotes an awareness and commitment to safeguarding throughout the school community.
- Ensures that E-Safety education is embedded across the curriculum.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident.
- To ensure that an E-Safety incident log is kept up to date.
- To facilitate training and advice for all staff liaises with the Local Authority and relevant agencies.
- Is regularly updated in E-Safety issues and legislation, and be aware of the potential for serious child protection 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 and use of social media
- To ensure that the school follows all current E-Safety advice to keep the children and staff safe.
- To Review and update the E-Safety policy annually based on evolving threats and technology trends.

Staff:

Are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement.
- They report any suspected misuse or problem to the Administrative Coordinator for investigation / action.
- All digital communications with students / parents / staff should be on a professional level and only carried out using official school email account.
- 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 and mobile devices 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.
- Incorporate lessons on digital wellness, screen time balance, and online ethics across subjects.

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy/Agreements.
- 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. 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.
- Should participate in annual E-Safety training and complete digital citizenship modules.

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 parental engagement both by informing and involving them. Parents and caregivers will be encouraged to support the school in promoting good E- Safety practice and to follow:

- The guidelines of Acceptable Use Policy/Agreement.
- Usage of digital images/video.

Parents are invited to attend school workshops on E-Safety and digital parenting.

2.3. ACCEPTABLE USE POLICY

This policy has been designed to ensure safe and responsible use of digital devices, computer networks including internet, and other online resources by all stakeholder of school community. We envision a learning environment where technology is a part of us, not apart from us. The school is committed to promote and safeguard the welfare of all students and an effective online safety strategy is paramount to this.

PURPOSE:

- To encourage safe and responsible use of digital devices, computer networks including internet, and other online resources the by both students and staff working within our school.
- To encourage the development of skills to access, analyze and evaluate resources from the internet.
- To use these resources to support teaching and learning across the curriculum.
- To ensure their supervised and appropriate use.

This policy will be communicated to students/staff/parents in the following ways:

- Policy to be posted on the school website/ staffroom.
- Policy to be part of school induction pack for new staff.
- Acceptable use agreements to be discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school.

Acceptable Use Agreements will be reviewed annually and re-signed by all users to reflect current digital risks.

Please refer to Acceptable Use Policy Agreements for students, staff and parents of School of Knowledge.

2.4. WHOLE SCHOOL

At School of Knowledge, we prioritize on the safety of all stakeholders. All the school policies are aligned with E-Safety policies. It is very important for the school community to be consistent in online safety approaches through variety of media and activities that provides whole school input.

Please refer to Whole School Policies of School of Knowledge:

1. *Behaviour Policy*
2. *Anti-Bullying Policy*
3. *PHSE Policy*
4. *Child Protection / Safeguarding Policy*
5. *Computing Policy*

E-Safety is reinforced during school assemblies, parent-teacher meetings, and co-curricular programs.

2.5. STRATEGIES FOR MANAGING UNACCEPTABLE USE

1. Responsibilities of Stakeholders

Parents:

Parents play an integral role in helping their children use their technology effectively and safely. The following tips will be disseminated to parents at the outset of the academic year.

1. Know your child’s password and screen names for all electronic devices.
2. Be aware what your child writes on his or her electronic device(s). Parents should carefully monitor the family computer as well.
3. Attend school or community functions where cyberbullying is being discussed. Talk with other parents and your child’s teacher and school counsellor if you suspect your child is involved in cyberbullying.
4. Watch for any sudden or ongoing signs that your child seems anxious, fearful, withdrawn, uninterested in school or being with former friends.
5. Remind your child to treat others the way he or she would like to be treated. That means never saying or writing anything about another person that they would not say be willing or comfortable saying to that person’s face.

Teachers:

Teachers must help prevent cyberbullying from happening by establishing, at the outset, boundaries and expectations of how students are to behave and stay safe online and offline. By discussing acceptable use policy with students, rules and consequences in case of violation will be made clear to them. In the event of violation, teachers can use the following strategy for handling it:

1. Observation and Intervention: Pay attention to the behaviour of students and potential conflicts. Intervene as necessary. Ask questions and listen to both what is being said and what is not.
2. Documentation: Take notes when incidents occur, no matter how minor they seem. Seemingly small things can quickly explode into major conflicts. Also, if a student directly reports cyberbullying to you or you witness an occurrence, encourage them to save any evidence.
3. Communication: Verbal and/or written communication with the administration about the incident(s) should happen as soon as possible. Be sure to provide any documentation of any previous incidents, conversations, or observations.
4. Solutions: Solutions to cyberbullying should always be in the interest of protecting students and should center on the targeted student.

Teachers will use structured reflection tools after E-Safety incidents to help students learn from mistakes.

2. Procedures for Dealing with Cyberbullying Offences

For any violation, appropriate disciplinary action will be taken consistent with the provision in the School of Knowledge Behaviour Management. There is a procedure to deal with cyber bullying internally, but if needed, students are encouraged to contact the Child Protection Center Hotline #11611, Ministry of Interior, UAE or email to childprotection@moi.gov.ae .

3. Handling Misuse/Complaints

School of Knowledge will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile devices. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access. The following guidelines are followed an enforced to mitigate misuse.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by teacher.
- Informing parents or careers.
- Removal of Internet or computer access for a period.
- Referral to Pastoral Care/Well Being Team.

Any complaint about staff misuse is referred to the Admin Coordinator in conjunction with the E- Safety Officer. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school Child Protection/Safeguarding Policy.

4. Expected Conduct

In School of Knowledge, all users:

- Are responsible for using the school computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems.
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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.
- Are regularly updated on emerging digital threats and evolving responsibilities in technology use.

2.6. MANAGING DIGITAL CONTENT

Social Media Guidelines:

School of Knowledge blocks/filters access to social networking sites or newsgroups. Students are given tools and information to understand the advantages and disadvantages of social media usage during their e-Safety Education Programme. Staff are prohibited from hosting school related images/videos on their personal social media and understand that interacting with a student on social media is a serious offense that is likely to result in severe consequences. Expectations are clear:

- Staff must not add pupils as friends in social networking sites.
- Staff must not post pictures of school events on personal social networking sites such as Facebook, Instagram, Twitter etc.
- Staff must not use social networking sites within lesson times.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils' parents/ careers or school staff.
- Data about pupil/ staff or parents is not shared on social media. They do not engage in online discussion on personal matters relating to members of the school community.
- Staff must immediately report accidental breaches of social media policy to the Admin Coordinator.

Annual digital safety workshops will reinforce guidelines for ethical and professional social media conduct.

School website:

- The website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorizer- IT Administrator
- Student personal data on the website will be anonymized unless prior consent is obtained.
- Website updates are logged and subject to monthly administrative review.

Use of Digital and Video Images:

At School of Knowledge, we prioritize on the safety of our students be it Face to Face learning or Distance Learning. E-Learning involves taking a lot of photographs and video recordings of students either as individual or in groups. This in turn are uploaded in various forums such as school displays, school publicity material, school website, school newsletter, Facebook and YouTube. Media taken for school use is stored securely on encrypted drives. Staff must ensure that students in "No Photograph" consent categories are excluded from public visuals.

Parental permissions are gained when publishing personal images on the school website, newsletter, social media and other publications.

Please refer to Parental Consent Form for Student's Photograph/Video Usage of School of Knowledge.

2.7. MOBILE DEVICE*

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 (Bring Your Own Device) 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 Policy/Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the schools normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Students receive training and guidance on the use of personal devices.
- 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.

Please refer to BYOD Policy of School of Knowledge.

(*Applicable only if the students are asked to bring their own devices)

2.8. REPORTING

Escalation process for E-Safety incidents:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school’s escalation processes.
- Support is actively sought from other agencies.
- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school’s senior leaders.
- Parents/guardians are specifically informed of e-safety incidents involving young people for whom they are responsible.

As part of the E-Safety Education program, students and parents alike are well informed that their Class Teacher is their first point of contact to report any online behavioral or technological issues. The Class Teacher is then responsible for notifying the necessary parties, namely, the Admin Coordinator, E-Safety Team or the IT Department. All such reports are logged in the relevant respective log books.

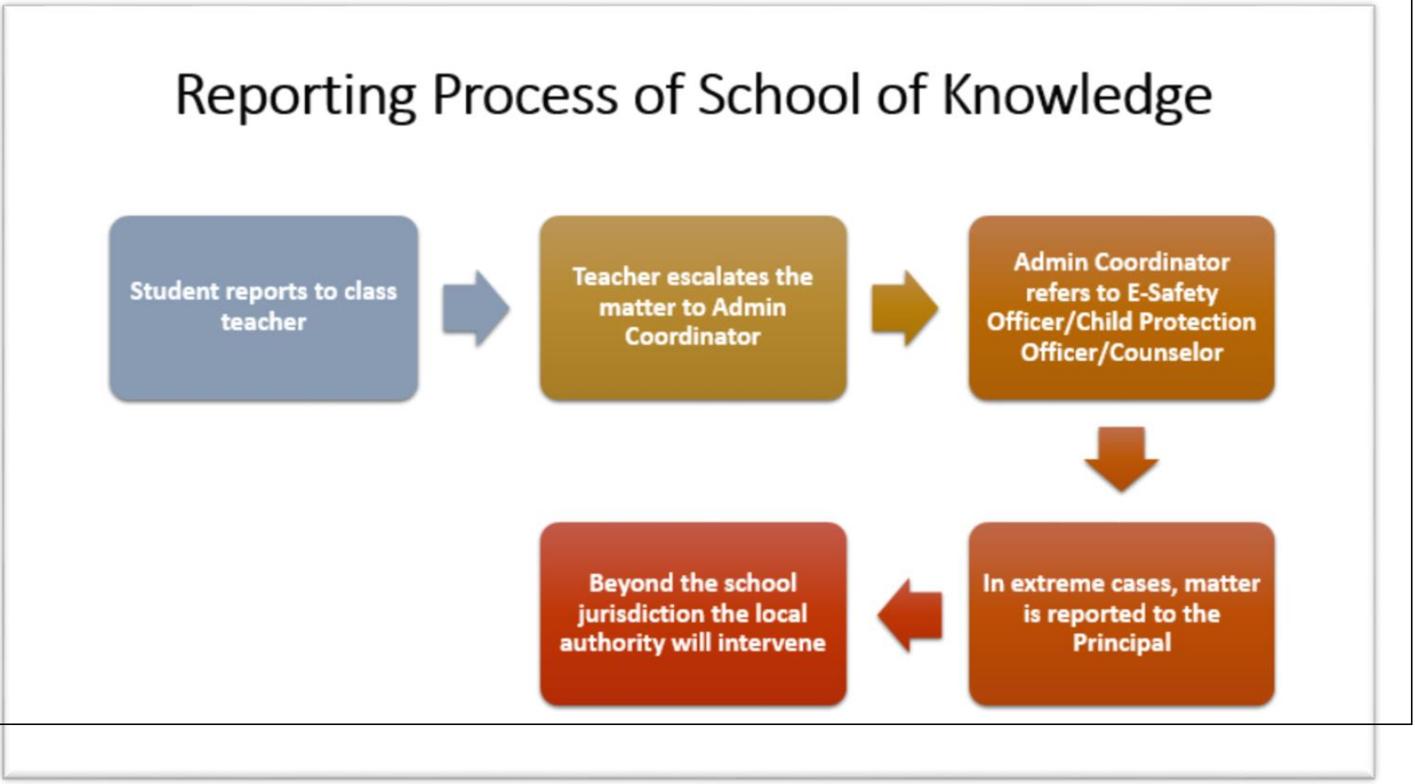
Reporting Cyberbullying:

The following guidelines have been provided to teachers to encourage their active role in the reporting process of cyber-bullying:
Support – Provide the student being bullied with support and reassurance. Tell them that they did the right thing by telling. Encourage the child to get help from parents, the E Safety Officer, Principal, School Counsellor or Teachers.

1. ***Evidence*** – Help the child keep relevant evidence for investigations. This can be done by taking screenshots, printing web pages. Do not allow the deletion of messages.
2. **Inform** – Give the child advice for making sure it does not happen again. This can include changing passwords or contact details.
3. ***No Retaliation*** – Ensure that the student does not retaliate or reply to the message.
4. ***Privacy*** – Encourage the child to keep personal information private on the internet.
5. ***Investigation*** – The cyber bullying claim needs to be investigated fully. If the perpetrator is known, ask them to remove offending remarks or posts. All records should be kept as part of the investigation.
6. ***Guidelines***- Any violation of the student rules including bullying prohibition will be referred to Behavior Management.

Reporting Process:

The consequences of E-Safety incidents will cover a range of challenges, with consequences that range from those that may appear trivial to serious abuse and loss of life. This means we must ensure that we treat all reports with appropriate professionalism and follow correct and agreed procedures



Reporting Process of School of Knowledge

Student reports to class teacher

Teacher escalates the matter to Admin Coordinator

Admin Coordinator refers to E-Safety Officer/Child Protection Officer/Counselor

In extreme cases, matter is reported to the Principal

Beyond the school jurisdiction the local authority will intervene

2.9. . PROFESSIONAL STANDARDS

At School of Knowledge, the appropriate use of technologies for teaching and learning process are vital to our school's functioning. To ensure a quality teaching-learning experience when planning and delivering, the following Online Platforms support Distance/Hybrid Learning. Staff/student/parents must be used according to set professional standards:

1. Google Workspace (formerly G Suite) : All Google Workspace plans provide a custom email for our organization (St. Mary's Group of School- **smgeducation.org**) and includes collaboration tools like Gmail, Calendar, Meet, Chat, Drive, Docs, Sheets, Slides, Forms, and more.

2. Learning Management System:

- Google Classroom: The primary purpose of Google Classroom is to streamline assignments, boost collaboration, and foster communication. Classroom is available on the web or by mobile app. You can use Classroom with many tools that you already use, such as Gmail, Google Docs, Google Slides, Google Forms and Google Calendar. Used for cohort (Year 2-Year 8). Staff/Students accesses it with given **SMG** account by the IT administrator of our school.
- Mograsys: It is used for the administration, tracking, reporting, automation and delivery of educational courses. Attendance, Marks-Entry for Grade book and Communication with parents/staff/students is upheld through Mograsys. Staff/Students/Parents accesses it with given username and password by the IT administrator of our school.

3. Video Conferencing Tool:

- Google Meet: It is used for cohort (Year 2-Year 8) for live sessions through Google Classroom. Meet uses the same protections that Google uses to secure information and safeguard privacy. Meet video conferences are encrypted in transit, and array of safety measures are continuously updated for added protection. It is used for cohort (Year 2-Year 8) for live sessions through Google Classroom.
- Zoom: It is used for FS2 and Year 1 for live sessions under the supervision of careers. Year 2-Year 8 uses Zoom for mass assembly through **smgvideoconfernce** gateway. All virtual school events takes place through Zoom by using **smgvideoconfernce** domain.

4. Other Applications:

- Active Learn: A digital learning space from Pearson Education for the pupils and a toolkit for teachers, so that teacher can search, plan, allocate and assess all in one place. It is used across FS2 to Year 8. Active Learn Primary is used for English, Mathematics and Science.
- Live Worksheets: Live Worksheets allows to transform the traditional printable worksheets and

classwork (doc, pdf, jpgs) and turn them into interactive online exercises with automatic grading, making them... live and easy to use.

- Google Form: It is used for assessment and evaluation. When used for assessment it's been restricted to SMG users only.

All other apps used for teaching and learning are accessed by using SMG username (Log in with Google for education). For any tech related matters, we encourage teachers, students, and parents to contact the IT administrator at mis-sok@smgeducation.org

5. Online Etiquette

The use of the electronic platforms via the internet facilitates creation and communication of information. It provides opportunities for social interaction. However, communication is different from a face-to-face setting. Words or images could be misunderstood. Hence, it is extremely important to observe online decorum.
To ensure that the message being conveyed will be received correctly, and to prevent any improper and harmful use of the technology, School of Knowledge community members must adhere to the following guidelines:

1. Be respectful. – Always keep in mind the feelings and opinions of others, even if they differ from your own. Anything you cannot say face-to-face, don't do it online. Criticizing somebody, writing against someone, or anything that violates the honor or dignity of the person is a serious offense. Always use appropriate language and graphics.
2. Grammar and spelling matter. – In an educational setting all written communication must be formal and should reflect proper writing style.
3. Avoid inappropriate material. – Using electronic gadget to make, distribute, or redistribute jokes, stories or images that are harmful to the dignity of a person, or stereotypes or labels relating to race, gender, ethnicity, or religion will result to disciplinary action. Don't forward chain letters or unimportant emails to others. They will only fill up their mailboxes.
4. Be aware of strong language, all caps, and exclamation points. – Written texts can be misread and misunderstood. Typing in caps is considered screaming online. Besides it takes longer time to read a text that is typed in all caps. Think before you hit the SEND button.
5. Consider other's privacy. – Ask for permission if you want to forward someone's email. No image of any student will be posted online without the knowledge and permission of the parents. Only wholesome and decent photos are to be published.
6. Cite your sources. – Always acknowledge the author of any idea that you use or share if this idea does not come from you. In a formal writing the sources are listed under References. Presenting someone else's work or ideas as your own, with or without their consent, by incorporating into your own work without full acknowledgement is called plagiarism. It is illegal.

6. Email Protocol and Email Use Policy

All staff to adhere to school's Email protocol and email use policy. School of Knowledge commits to:

- Provide staff with an email account for their professional use and makes clear personal email should be through a separate account.

- Educational apps utilized are verified as safe platforms for school usage and is been accessed by using SMG account (Log in with Google for Education).
- Ensuring that email accounts are maintained and up to date.
- Reports messages relating to or in support of illegal activities to the relevant Authority.
- Knows that spam, phishing and virus attachments can make e-mails dangerous.

All students have been taught about the safety and 'netiquette' of using e-mail both in school and at home. They are taught:

- not to share out their e-mail address and password;
- they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
- to 'Pause and Think Before They Click' and not open unknown attachments;
- that they must immediately tell a teacher / trusted adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;

Staff understand:

- Never use personal email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organization must be written carefully and may require authorization.

3. INFRASTRUCTURE

3.1. PASSWORD SECURITY:

The school will be responsible for ensuring that the school data and network is as safe and secure as they have their own username and password and 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 agreements.
- 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 digital system including school account email and Virtual Learning Environment like Google Classroom, Google Meet, Active learn.

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

Length recommend a minimum of six (preferably eight) characters in a password for students and regular users and a minimum of fifteen characters for 'secure data users.' The reason for this is because the time one takes to crack a password increases exponentially with its length.

Complexity

Passwords should contain at least one alpha, one numeric and one non-alphanumeric character (a symbol). Complexity is, however, a double edged sword because if you are using just six characters, only 27% of the total possible passwords would meet the complexity requirement.

Repetition

This disallows use of a certain number of previous passwords. It is used to ensure that a user does not keep using two passwords over and over again by alternating between them. If this was set to five, then one would not be able to use any of their previous five passwords.

Forced Changes

Password changes may also be forced by the system at regular time intervals. For regular users, an interval of a year is generally good enough, but secure data users should probably be asked to forcibly change their password two to four times a year. If the change frequency is low, compromised passwords have a higher value, but if the frequency is too high, it is more likely that users will take steps that make their personal password management easier, such as writing passwords down on post-it notes which nullifies any intended benefit of a frequent change. Never share passwords with other employees, including your assistant. If a group of people need access to the same files or applications, they should be granted that access with their own login.

3.2. FILTERING:

The school will be responsible for ensuring that the school infrastructure / network / filtering 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 IT administrator is effective in carrying out their E-Safety responsibilities:

- There will be regular reviews and audits of the safety and security of school academy technical systems.
- 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 Policy/Agreement.

The following is filtered:

- ✓ Social media networking sites (Facebook, Instagram and Twitter)
- ✓ Gaming sites
- ✓ Streaming sites
- ✓ Pornography and sexual harassment sites
- ✓ Any sites related to violence
- ✓ VPN /Client VPN
- ✓ Unwanted download is blocked with threat and malware download blocker
- ✓ Other blocked websites except educational sites

Please refer to Filtering Policy of School of Knowledge.

3.3 TECHNICAL SECURITY:

School of Knowledge strives for the utmost technical security at each step. We:

- Provides secure network connection to staff and students.
- Has additional local network auditing software installed.
- Ensures the E-Safety team is up-to-date with services and policies

We ensure to protect the school network and systems from all threats, internal, external, deliberate or accidental. The policy is aimed at:

- ✓ Safeguarding the availability, confidentiality and integrity of the school's information.
- ✓ Protecting the IT assets and services of the school against unauthorized access, intrusion, disruption or other damage.
- ✓ Ensuring compliance with applicable regulations of MOE and SPEA.
- ✓ Providing a governance structure with clear lines of responsibility and accountability.
- ✓ To provide a mechanism to establish procedures to protect against security threats and minimize the impact of E-Safety incidents.

Please refer to Technical Security Policy of School of Knowledge.

3.4 PROTECTING PERSONAL INFORMATION:

School of Knowledge gathers, collects and uses information regarding our students, staff, and parents. This information must be collected, handled and stored to the full extent of the UAE's Data Protection Laws. As such, at this school:

- Staff to report any incidents where data may have been breached.
- We ensure all staff sign an Acceptable Use Agreement form. We have a system so we know who has signed. This makes clear staffs' responsibilities with regard to data security, passwords and access.
- We require that any Protect and Restricted material must not is to be removed from the school and limit such data removal.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- All servers are in lockable locations and managed by IT administrator.
- We lock any back-up tapes in a secure cabinet.

Please refer to Data Protection Policy of School of Knowledge.

4. EDUCATION:

School of Knowledge has a clear curriculum and outline of lessons for students regarding important topics such as online safety, stranger danger, plagiarism, sharing of personal information, and more.

4.1. ONLINE SAFETY EDUCATION PROGRAMME & DIGITAL CITIZENSHIP

School of Knowledge has a clear, progressive e-safety education programme as part of the primary curriculum. This covers a range of skills and behaviors appropriate to their age and experience, including:

- To understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour;
- Keeping personal information private;
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos;
- To understand why they must not post photos or videos of others without their permission;
- To know not to download any files – such as music files - without permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand the impact of cyberbullying and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyberbullying and how to seek help if they experience problems when using the internet and related technologies, i.e. teacher or parent.

School of Knowledge plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas. Teachers will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign.
School of Knowledge commits to:

- Ensuring staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensuring that when copying materials from the web, staff and pupils understand issues around plagiarism.
- How to check copyright and also know that they must respect and acknowledge copyright.
- Ensuring that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in popups; buying on-line; on-line gaming.

Please refer to Online Safety & Digital Citizenship Curriculum Plan of School of Knowledge.

4.2. CONTRIBUTION OF YOUNG PEOPLE:

School of Knowledge has elected E-Safety monitor from each class from Years 2 to Year 8; these will be different each month on a rotation basis. Each child will be given guidelines on how to ensure online safety is practiced in each of their lessons and show themselves to their peer as a leader on all matters related to online safety. Each student will receive further training and be granted a certificate.

A student council is a group of students from within the school elected to represent their fellow students. At School of Knowledge, we aim to develop in the school, opportunities for leadership and service to the school community. Safe and secure access to the internet has been never more important than today when our young ones are introduced to the internet for their studies. At School of Knowledge, we have a series of assemblies to acquaint students with E-Safety addressed by the Prefects. True to the concept, all assemblies headed by the prefects and guided by teachers. The assemblies met the criteria set out to promote awareness of the do's and don'ts in surfing the web for knowledge, research, and using the various apps responsibly without revealing too much information to an unknown world that lies ahead. Students are cautioned about cyber-bullying, phishing, cloning, duplicating identities and the deep web.

4.3 STAFF TRAINING:

School of Knowledge will provide several training opportunities whereby staff will learn best practices in online safety. We ensure:

- Ensure staff have had training and know how to send or receive sensitive and personal data.
- Makes regular training available to staff on e-safety issues.
- Updates are done in staff meetings.
- Provides, as part of the induction process, all new staff with information and guidance on the E-Safety Policy and the school's Acceptable Use Policies.
- All staff enrolling and taking the E-Safe Courses form Sharjah Educational Academy.

4.4 PARENTAL ENGAGEMENT:

We at School of Knowledge ensure that along with pupils, the parents are also aware of information and education about online safety. Clear routes have to be provided for effective communication and to online learning. In this regards school has already drafted Acceptable Use Policy wherein the descriptor for online safety is been provided and parents have acknowledge and signed the policy.

Parental engagement not only informing by sharing information but actively involve parents in being part of educating students about E-Safety. School has taken an initiative to conduct workshops organized by the Parents Council members on the topics related to online safety. Apart from this information supporting online safety is provided through various materials. Follow up is done based on the material sent by conducting surveys to gage the understanding. This survey responses are analyzed and evaluated by E-Safety team and SLT for further enhancement.

Please refer to Parental Engagement program of School of Knowledge.

5. IMPACT AND MONITORING

The E-Safety policy is referenced from within other school policies: Anti-Bullying policy, Child Protection/Safeguarding, PSHE Policy and Computing Policy. For impact and monitoring purposes, School of Knowledge has formed E-Safety Team who regularly meet to discuss the efficiency of their programs and policies. Some key points to note:

- The E-Safety policy will be reviewed bi-annually or when any significant changes occur with regard to the technologies in use within the school.
- The e-safety policy has been written by the school E-Safety Team and is current and appropriate for its intended audience and purpose.
- All amendments to the school E-Safety policy will be discussed in detail with all staff.
- The evaluation is based on the incident and behaviour log and the surveys which will be conducted for all stakeholders.

POLICY REVIEW LOG:

Policy Details	**E-Safety Policy**
Reviewed/ Approved By & Date	**E-Safety Team and SLT / June 2025**
Next Revision Date	**June 2026**