E-Safety Policy

Policy Statement

Rationale

It is the duty of the school to ensure that children and young people are protected from potential harm both within the school and beyond. The e-safety policy applies to all members of the school community and is to be adhered to by all (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of the school's ICT systems, both in and out of school. Should there be an incident of cyber bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school, the school will impose disciplinary penalties for inappropriate behavior where this is reasonable as stipulated in the school's behavior policy.

The school will deal with such incidents within this policy and associated behaviors and will, where known, inform parents / carers of incidents of inappropriate e-safety behavior that takes place out of school.

Aims

- To emphasize the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring their input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

Definitions

The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

Designated Roles and Procedures

Governors and Principals

It is the overall responsibility of the Principals to ensure the Governors understand their responsibility and to have an overview of e-Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:

- The Principal has designated an e-Safety officer to implement agreed policies, procedures, staff training, curriculum requirements and to take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. All staff and students are aware of the person who has been appointed to this role within the school.
- There is a standard disclaimer on all emails stating that the views expressed are not necessarily those of the school or organization.
- Resources should be provided for the e-Safety officer to be trained with up to date information in order for them to update policies, where appropriate.
- All staff are responsible for promoting e-Safety across the curriculum.

E-Safety Officer

It is the role of the designated e-Safety officer to:

- ❏ Promote the importance of e-safety within school as part of its duty of care to ensure the safety of their pupils and staff.
- ❏ Establish and maintain a safe ICT learning environment within the school.
- ❏ Ensure that the Acceptable Use Agreements are reviewed annually, with up-to-date information, and that training is available for staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- ❏ Work alongside the Network Manager to ensure that filtering is set to the correct level for staff, children and young people.
- ❏ Equip (i.e. training) children to stay safe online, both in school and outside of school.
- ❏ Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- ❏ Liaise with the Cyber Safety PLC to discuss and mitigate e-Safety trends or threats identified within the school so that policies and procedures are up-to-date to take account of any emerging issues and technologies.

- ❏ Update staff about new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- ❏ Oversee transparent monitoring of the Internet and online technologies. The school's Internet firewall system also provides a high level of transparent monitoring as part of its functionality.
- ❏ Regularly analyze the e-Safety incident logs to help inform future development and safeguarding, where risks can be identified.
- ❏ Work alongside the Network Manager to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- ❏ Ensure that unsolicited emails to a member of staff from other sources are minimized.
- ❏ Advise on the e-Safety curriculum review to ensure it is up-to-date to take account of any emerging issues and technologies.
- ❏ Provide regular reports to the Senior Leadership Team.

E-Safety Officer - Job Description

- ❏ Developing an e-safety culture under the direction of the management team and acting as a named point of contact on all e-safety issues.
- ❏ Ensuring that everyone including children and young people know what to do if they are concerned about an e-safety issue.
- ❏ Ensuring that e-safety is embedded within continuing professional development (CPD) for staff and co-ordinating training as appropriate.
- ❏ Ensuring that e-safety is embedded across the curriculum and in all concerned activities as appropriate.
- ❏ Ensuring that e-safety is promoted to parents and carers, other users of ICT within the Liwa community.
- ❏ Ensuring that adequate resources are provided to all pupils to support them in their understanding of all issues concerning e-safety..
- ❏ Maintaining an e-safety incident log.
- ❏ Monitoring and reporting on e-safety issues to the management team, and other agencies as appropriate.
- ❏ Developing an understanding of the relevant local and national guidance.
- ❏ In consultation with the SLT, liaising with the local authorities as appropriate.
- ❏ Reviewing and updating e-safety policies and procedures on a regular basis and after an incident.
- ❏ Ensure that learning outcomes and feedback are appropriately shared.

- ❏ Ensuring that the infrastructure and technology provides a safe and secure environment for all within the Liwa community.
- ❏ Ensure that the school has Firewalls.
    - ❏ Anti-virus and anti-spyware software.
    - ❏ Filters.
    - ❏ Awareness of any wireless technology issues.
    - ❏ A clear policy on using personal devices.

Cyber Safety Professional Learning Committee.

It is the responsibility of the committee within the school to:

- ❏ Review all policies and protocols pertaining to E-Safety.
- ❏ Ensure all the school has an E-Safety training programme
- ❏ Ensure teachers implement cyber safety lessons into their ongoing lessons.
- ❏ Ensure the school environment is safe and secure and that appropriate safety protocols are in place.
- ❏ Plan regular community events related to e-safety.

Data Protection Officer

It is the role of the designated e-Safety officer to:

- ❏ Providing training on compliance requirements
- ❏ Provide training to staff involved in data processing
- ❏ Conducting audits to ensure compliance and address potential issues proactively
- ❏ Serving as the point of contact between the school and the regulatory authorities.
- ❏ Monitoring performance and providing advice on the impact of data protection efforts
- ❏ Maintaining comprehensive records of all data processing activities conducted by the school, including the purposes of all processing activities, which must be made public on request
- ❏ Interfacing with data subjects to inform them about how their data is being used, their right to have their personal data erased, and what measures the company has put in place to protect their personal information.

Data Protection : Job Description

- ❏ An understanding of the Data Protection Law (contents and interpretation) and how this is applied and aligned to the school's data protection policy.
- ❏ Interpreting regulatory requirements and providing advice on how this could be applied within the school.

- Liaising with external counterparts (regulators) as well as internal stakeholders to support in the implementation of the school's data protection policy in compliance to the UAE law.
- Provide data protection awareness staff training to all stakeholders.

E-Safety Data Monitoring Officer

It is the role of the designated e-Safety officer to:

- Establish and coordinate the e-safety monitoring system including data collection, analysis and review.
- Identify appropriate e-safety infringement indicators, how these are monitored and reviewed.
- Work closely with the relevant teams (Network Administrator, E-learning Co-ordinators and Device management team) to prepare specific data collection methods and tools
- Coordinate monitoring activities and inputs required of other team members.
- Anticipate, plan and support reporting requirements.
- Ensure information gathered through monitoring activities is shared quickly and in an appropriate format with the E-Safety Officer so that any problems arising can be addressed.

Staff and Adults

It is the responsibility of all adults within the school to:

- Check that the filtering levels are appropriate for pupils and are set at the correct level and to report any concerns to the e-Safety officer.
- Alert the e-Safety officer of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that all pupils are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner. All pupils should know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Report accidental access to inappropriate materials to the e-Safety officer in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school/education setting or other establishment's network.

- ❏ Ensure that all sensitive information is only stored on the school's network and can only be accessed by authenticated users within the school domain as stated in the data protection policy. (No sensitive data should be saved on local drives or personal storage devices.)
- ❏ Report incidents of personally directed "bullying" or other inappropriate behavior via the Internet or other technologies to the e-Safety officer.
- ❏ Be aware that by submitting the school policy's online form you are agreeing to be bound by the terms of the policy.
- ❏ Be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- ❏ In lessons, where internet use is pre-planned, students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

It is the responsibility of all pupils within the school to:

- ❏ Be responsible users of the school ICT systems in accordance with the school's Acceptable Use Policy.
- ❏ To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- ❏ To understand the school policies on the use of mobile phones, digital cameras and hand-held devices. (policies on the taking / use of images and on cyber-bullying.
- ❏ Adopt 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.
- ❏ Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Guests/Visitors

It is the responsibility of all guests within the school to:

- ❏ Understand that Guests are not given access to the school systems except WiFi.
- ❏ Use the school's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to Pupils' safety or to the safety and security of the systems, devices and other users.
- ❏ Report accidental access to inappropriate materials to the e-Safety officer in order that inappropriate sites are added to the restricted list.

Operational Implementation

Education - All Students

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

E-Safety education will be provided in the following ways:

- A planned e-safety program is provided as part of the ICT curriculum and through PACE (Personal and Community Education).
- The curriculum is regularly re-visited to cover both the use of ICT and new technologies in school and outside school. Key e-safety messages are reinforced as part of a planned program of assemblies and tutorial / pastoral activities.
- Students are 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 are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems / internet are posted in all rooms.
- Staff are required to act as good role models in their use of ICT, the internet and mobile devices.

Education & Staff Training

It is essential that our staff receive e-safety training and understand their responsibilities, as outlined in this policy:

- E-safety training for staff is provided as part of our induction program at the beginning of the school year and throughout the course of the year as required.
- All staff are regularly updated with relevant e-safety developments
- This E-Safety policy is presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Officer will provide advice / guidance / training to individuals as required.

Education - Liwa Community

We value the contribution that the wider community makes in ensuring that our students are safe, as such we will continue to support the wider Liwa community in all matters relating to e-safety.

- ❏ Regular updates will be provided to parents on current e-safety threats and how they may protect themselves and their families.
- ❏ Basic e-safety training will be provided on how to secure accounts and set/check privacy settings.
- ❏ Regular updates/reminders on how to report any issues/concerns regarding e-safety in the school.
- ❏ Advice on how to monitor or manage what their children are doing online including managing screen time.

The Curriculum

- ❏ Cyber security and ethics is a key component of the ICT curriculum for all Grades (K-12), key competencies covered ensure progression across the grades and are aligned to expected grade outcomes.
- ❏ E-safety is a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of technology across the curriculum.
- ❏ In lessons, where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use.
- ❏ Most sites are blocked by default by the Network filtering and a request must be made by the teachers so that access is given to the students. All sites are examined before permission is granted.
- ❏ Where students can freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites young people visit.
- ❏ Students should be taught in all lessons, to be critically aware of the materials / content they access online 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.

Password Policy Implementation

Staff and Students' Passwords

1. All users are issued with a **password when the email is initially created and shared.**
2. Emails currently created for all students KG-12 and staff.
3. Once the account is created, **users are immediately asked to change their password.**

4. The recommended strength and accepted criteria for the password is suggested by the system; **passwords that do not meet the criteria are not accepted.**
5. In the case of a forgotten password or a need to reset the password if this has been compromised then a **request for a password reset by the parents to the school** using the school's communication channels is sent to request the reset. The new password is then shared with the parent that has requested the reset.
6. Staff can request the information directly from the IT team by calling them on the school's support telephone number.
7. **The password refresh will be applied twice a year for all students Grade 3-12 and every 90 days for staff.**
8. **All passwords for KG-Grade 2 students** will be set once a year and all passwords will be communicated to the parents by the class teacher via the Schools communication channel.
9. No database of the staff or students passwords are available, IT support only has the reset option.

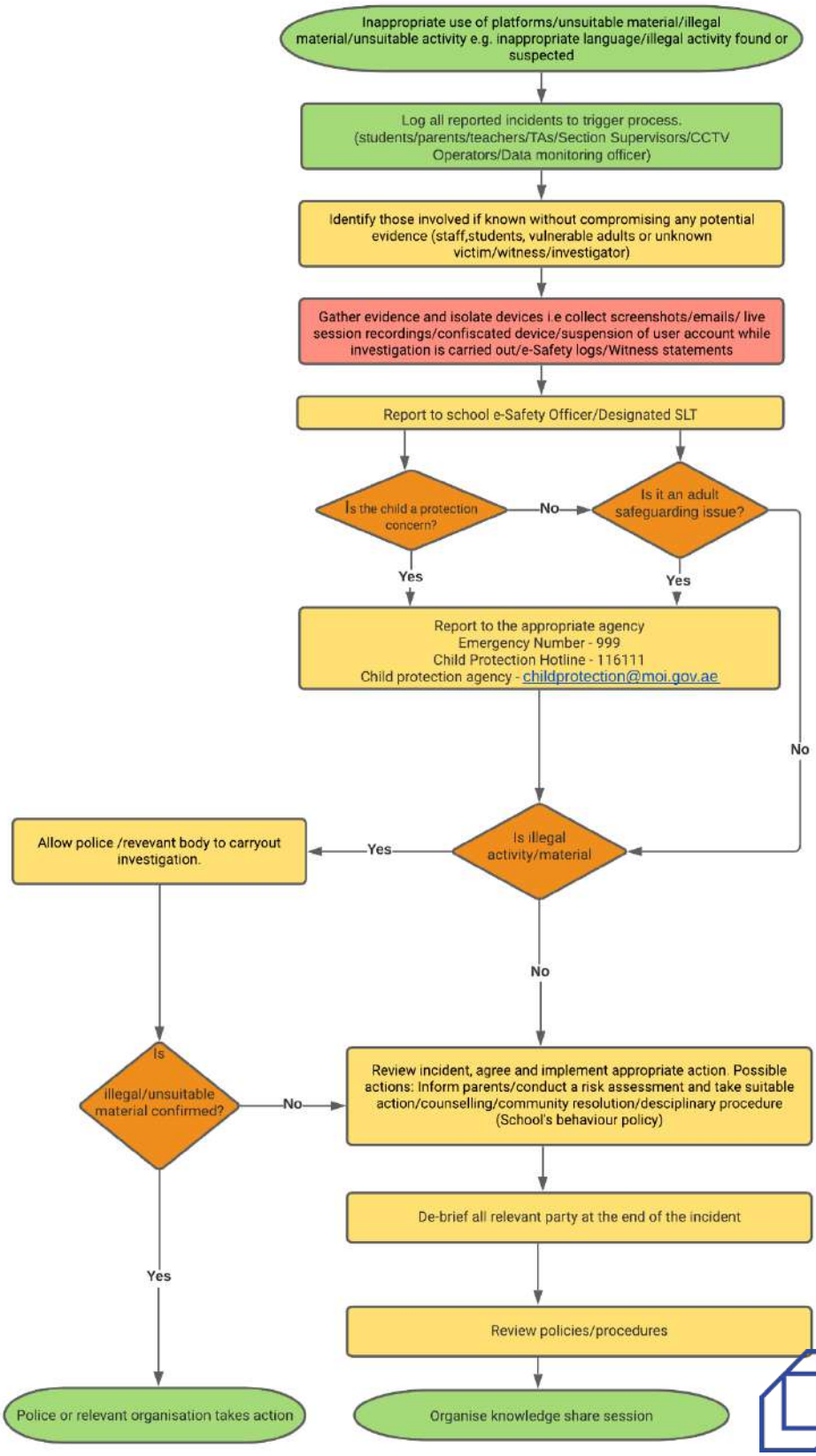
Guest/ Visitor's Access

1. Guests are not given access to the school's system (i.e. files and folders).
2. They are issued with a **temporary WiFi password** for internet access.
3. All user groups; students, staff and guests have a **separate SSID**.

Sanctions

1. The Principal, via the e-safety officer, will ensure that any misuse or incident has been dealt with appropriately, according to the school's behavior policy, and that appropriate action is taken.
2. Sanctions to be applied as appropriate include: suspension of an individual's internet access at School and/or suspension of an individual's user account for a period of time.
3. In serious cases (and where cyberbullying by an individual continues) the Principal may decide to exclude from School the person or persons responsible.
4. Through regular communication between the e-safety officer, social workers and teachers, it is hoped that any pupil who either seems to be a victim of cyberbullying or is repeatedly being a cyberbully will be quickly identified.
5. When it is deemed necessary, by the social worker, written accounts will be required from all those involved. The social worker will contact the parents of those pupils involved.
6. Should there be an incident of cyber bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school, the Principal can impose disciplinary penalties for inappropriate behavior where this is reasonable.
7. The school will deal with such incidents within this policy and associated behaviors and anti-bullying and will, where known, inform parents / carers of incidents of inappropriate e-safety behavior that takes place out of school.
8. Failure to adhere to the policy will be dealt with in accordance with the school's Rewards and Sanctions Policy, the School's Code of Conduct and when necessary the Child Protection Policy.

E-Safety Incident Report Procedure



Appendix

Federal Law No. 5 of 1985: The Civil Code

Federal Law No. 3 of 1987: The Penal Code ('the Penal Code')

Policy Review and Update

Author(s):	Liwa Schools - E-Safety Audit Committee
Review frequency:	Annually
Review Date:	1st August 2022
Date of Next Review:	1st August 2023