

E-SAFETY POLICIES AND PROCEDURES

Policy

Online safety policies provide insights into overall safety standards when technology is adopted in different domains of the school. This policy aims to show and implement appropriate and secure digital practices for all staff, teachers, learners and parents.

It is important that the use of the internet and ICT is seen as a responsibility and that learners, staff, and parents utilize it correctly and practice good e-safety. It is important that all members of the school community understand the risks associated with Internet access.

Objectives of the e-safety policy

- Protecting and educating learners and staff in their use of technology.
- Educating teachers/parents on their roles in safeguarding and protecting LWIS-CiS learners from the Risks Associated with the Internet and Online Social Networking.
- Putting policies and procedures in place to help prevent incidents of cyber-bullying within the school community.

Cyber-bullying Policy

Cyber-bullying is the use of electronic devices and the internet to send or post messages or images that may harm an individual or group.

Cyber-bullying will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behavior policy.

Procedure

- The LWIS-CiS Internet Network access is protected with FortiGate Firewall and designed expressly for learners' use. It includes filtering tailored to the needs of our learners. It prohibits viewing or downloading of any inappropriate material (offensive or immoral remarks, jokes or any other comments that may offend others based on physical or mental disability, age, religion, social status, political affiliations, and ethnicity).
- Social Media sites have been blocked for learner/staff access within school boundaries except for the digital media team.
- Teachers guide the learners in online activities that will support learning outcomes, depending on the learners' age and maturity.
- All learners and staff are educated on the importance of password security and the need to logout of accounts and not to open e-mails or attachments from unknown sources.

- The ICT classes' curricula include digital citizenship units designed to educate learners to be able to advocate and practice safe, legal, and responsible use of information and technology and exhibit leadership for digital citizenship.
- Online safety education is reinforced for all learners at every year level/ stage of learning.
- The school ensures that the personal information placed on the School's Internet and intranet is secure, even for a password-protected website.

Managing Information Systems

The school is responsible for managing the security of the computers and internet networks. It takes the protection of personal information very seriously. This means protecting the school network against viruses, hackers and other external security threats. The security of school information systems and users is regularly reviewed by the IT department. Here are some of the security measures the school takes to protect our computer systems:

- The school network is secured with Fortinet FortiGate firewall.
- The school computers are protected by Deep Freeze.
- The data stored on the school network is regularly checked for viruses.
- The use of strong user logins and passwords is enforced to access the school network.
- Portable media containing the school data or programs may not be taken off-site without permission.
- All systems, services and equipment used for storing data must meet acceptable security standards.
- Regular checks and scans are performed to ensure security hardware and software are functioning properly.

For more information on data protection in school, please refer to our **data protection policy**.

School Email Use

The school uses email internally for staff, teachers, learners, and externally to contact parents, suppliers...etc., and it is an essential part of school communication.

Scope

This policy applies to all members of the school (including staff, learners, parents, visitors) who will have access to and are users of the school digital systems, on campus and/or remotely.

Parents' Letter on E-safety in School:

Dear Parent(s)/Guardian(s):

This is to inform you that the school is using FortiGate Firewall to implement cyber safety measures to protect learners from cyber threats and ensure complete campus network protection. Accordingly, the ICT department is downloading Fortinet certificate on all learners' devices to maintain high-level network security.

Kindly note that your child/ward's device will not be affected by the certificate as it will be active only when on campus, i.e. connected to the school network.

Kindly note that removing the Fortinet certificate will disconnect your child/ward from the school network.

Regards,

The LWIS – CiS ICT Team