LITTLE FLOWER ENGLISH SCHOOL DUBAI

E- SAFETY POLICY

This policy & procedures are reviewed annually to ensure compliance with current regulations.

Approved/ Reviewed by	
Policy Lead	**MR. ABDUL**
Role	**IT COORDINATOR**
Date of review	**25-03-2025**
Date of next review	**25-03-2026**
Signature	

37

E- Safety Policy

Information and Communications Technology (ICT) covers a wide range of resources including; web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites

- Learning Platforms (MLE) and Virtual Learning Environments

- Zoom video conferencing

- Email and Instant Messaging

- Chat Rooms and Social Networking

- Blogs

- Video Broadcasting

- Downloading from the internet

- Gaming

- Mobile/Smart phones with text, video and/or web functionality

- Other mobile devices with web functionality

At LFES we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our school is **Abdul Mohamed**. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety coordinator to keep abreast of current issues and guidance through organisations such as CEOP and 'Think U Know'.

The e-Safety coordinator updates Senior Management Team and Governors. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and reviewing the e-Safety policy

This policy (for staff, governors, visitors and pupils), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: ICT, Home-school agreements, Behaviour, Health and Safety, Child Protection, and including Anti-bullying.

Our e-Safety policy has been agreed by the Senior Management Team and Staff. The e-Safety policy and its implementation are reviewed annually.

E-Safety skills development for staff

- All members of staff receive regular information and training on e-Safety issues through the coordinator at staff meetings.

- All members of staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

- All new members of staff receive information on the school's Acceptable Use Agreement as part of their induction.

- All members of staff incorporate e-Safety activities and awareness at the start of every term.

Community use of the Internet

- External organisations using the school's ICT facilities must adhere to the e-Safety policy.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach e-Safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies;
  i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Managing Internet Access
Information system security
- School ICT systems capacity and security will be reviewed regularly.
- Anti-Virus protection is updated regularly.
- System security is overseen by our IT regularly.

E-mail
- Pupils may only use approved e-mail accounts.

- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Published content and the school web site

The contact details on the school website are the school address, e-mail and telephone number. Staff or pupils' personal information is not published. The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Written permission from parents will be obtained before photographs of pupils are published on the school Website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

- Parentsmay withdraw permission, in writing, at any time.

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names will not be used anywhere on the school website, particularly in association with photographs.

- Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

Photographs taken by parentsfor personal use

In the event of parentswanting to take photographs for their own personal use, the school will demonstrate our protective ethos by announcing that photographs taken are for private retention and not for publication in any manner, including use on personal websites, e.g. School performances and assemblies etc.

Social networking and personal publishing

- The school blocks access to social networking sites.

- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate and or illegal (e.g. Facebook) for primary aged pupils.

- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Have deleted this

- Our pupils are asked to report any incidents of bullying to the school.

- School staff are advised not to add children, or parents as 'friends' if they use these sites.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.
- Pupils are not allowed to bring personal mobile devices/phones to school. Any phones that are brought to school are sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.
- Staff will use a school phone where contact with pupils is required.

Policy Decisions

Authorizing Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement (AUA) for pupils and abide by the school's e-Safety guidelines.
- Access to the Internet will be by directly supervised and to specific, approved on-line materials.
- All staff using a school laptop will be made aware of the schools Laptop Use Policy

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. The school will audit ICT provision to establish if the e-Safety policy is adequate and that its implementation is effective.

Handling e-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff and reported to the e-Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety coordinator
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints and concerns of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaint's procedure.

Communications Policy

Introducing the e-Safety policy to <u>pupils</u>

- E-Safety rules are displayed in the ICT suite and discussed with the pupils at the start of each term. All staff are aware that at least one dedicated e-safety lesson must be taught each term and at relevant points throughout

- Pupils will be informed that network and Internet use will be monitored.

- The school is vigilant when conducting 'raw' image search with pupils e.g. Google image

- Pupils are required to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme

<u>Staff</u> and the e-Safety policy

- Any information downloaded must be respectful of copyright, property rights and privacy.

- All members of staff are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- A laptop issued to a member of staff remains the property of the school (see laptop use policy). Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

<u>Parents</u> and the e-safety policy

- All parents, when their child joins the school, will be asked to sign the AUA for pupils giving consent for their child to use the Internet in school by following the school's e-Safety guidelines and within the constraints detailed in the school's eSafety policy.

- Parentsare required to make a decision as to whether they consent to images of their child being taken/used on the school website

- Parents are encouraged to look at the school's e-safety policy

- Parents receive an e-safety bulletin attached to the school newsletter at least once per term

The Learning Platform and other home/school internet use

- All staff have been trained and given advice on how to effectively use the zoom and google classroom
- Parents will be informed about what the zoom live class session and how it can enhance the learning of each child. All children will be given training on how to effectively use Google classroom and Socrative website
- All children will be given a username and password to access secure resources and facilities on the Learning Platform.
- Class teachers will monitor the use of the google classroom and Socrative website.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored on an annual basis by the e-Safety Coordinator.

This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the e-Safety Coordinator, Designated Child Protection Coordinator. Ongoing incidents will be reported to the full governing body.