LITTLE FLOWER ENGLISH SCHOOL DUBAI

CYBER SAFETY POLICY

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

Approved/ Reviewed by	
Policy Lead	MS. SEEMA
Role	ASST. SUPERVISOR
Date of review	25-03-2026
Date of next review	25-03-2027
Signature	

مدرسة الورود الصغيرة الانجليزية
LITTLE FLOWER
English School

CYBER SAFETY POLICY

Important terms used in this document:

(a) The abbreviation **'ICT'** in this document refers to the term 'Information and Communication Technologies.

(b) **'Cybersafety'** refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones

(c) **'School ICT'** refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below

(d) The term **'ICT equipment/devices'** used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, ipads, laptops, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), Gaming Consoles, and any other, similar, technologies as they come into use.

(e) '**Cyber bullying'**, is bullying which uses e-technology as a means of victimizing others.

Rationale

Cyber Safety encompasses technologies such as the Internet, and electronic communication devices including mobile phone, smart TV and other wireless technology.

LFES has an obligation to maintain a safe physical and emotional environment.

These responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cyber safety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

LFES places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

LFES recognizes that the presence in the learning environment of these technologies can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximize the benefits of these technologies, while at the same time to minimize and manage the risks.

LFES acknowledges the need to have in place rigorous and effective school cybersafety practices which are directed and guided by this cybersafety policy.

Policy

LFES will develop and maintain rigorous and effective cybersafety practices which aim to maximize the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimizing and managing any risks.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Policy guidelines

Associated issues the school will address include: the need for funding for cybersafety practices through inclusion in the annual budget, the review of the school's site improvement plan when necessary, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cybersafety for the school community and disciplinary responses appropriate to breaches of cybersafety.

Guidelines

1. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless they have been authorized to do so. This applies to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location.
2. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at LFES is to be limited to educational, professional development, and personal usage appropriate in the school environment.
3. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the school's computer/s and/or network facilities at all times.
4. The school has the right to audit at any time any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
5. Cyber safety depends on the effective practice by responsible ICT users (staff, students).
6. The safety of students is of paramount concern. Any apparent breach of cybersafety will be taken seriously. In serious incidents, advice will be sought from an appropriate source. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency who will take further action including confiscation and disposal of devices.
7. If students or parents/caregivers raise concerns about online bullying outside of school hours they will be encouraged to seek advice from social media platforms/police.

At LFES we take appropriate steps to protect our students

- Educating the students to use the equipment appropriately.
- Turn off the screen.
- Report immediately to the teacher any inappropriate materials
- Refrain from accessing inappropriate sites
- Should teachers or students encounter unsuitable material it will be reported to Administrator or IT as a matter of urgency.

Steps we take to protect students

- Use of a filtered service
- Supervision
- Planned activities
- Websites are previewed by teachers to ensure they are suitable for student's curriculum needs
- Teachers will choose the search engine
- Student use of email is supervised by an adult to make sure all emails are appropriate
- Students are taught to use the internet safely

Safety points for students

- Do not delete files or settings
- Ask permission before using the internet or a website
- Only send approved emails
- Do not give you names or address to anyone online
- Do not enter chat rooms
- Ask permission before taking anybody's photo
- If you see anything you do not like report it to your teacher
- **If you are bullied** don't ignore the bullying tell someone you trust, never reply, ask a teacher for help

Cyber Bullying

Cyber bullying is bullying through the use of communication technology like

- mobile phone text messages
- e-mails
- websites
- social media
- games

This can take many forms for example:

- Sending threatening or abusive/insulting comments through text messages, photos or e-mails, personally or anonymously
- Making insulting comments about someone for example on a website, social networking site

Some of the more common types of bullying are:

- Text messages
- Pictures/videos via mobile phone cameras
- Chat room bullying
- Mobile phone calls
- Emails
- Bullying via websites

Information for Parents: At LFES, we take this form of bullying seriously and will deal with each situation individually.

Technology allows the user to bully anonymously or from an unknown location, 24 hours a day, 7 days a week. Cyber-bullying leaves no physical scars so it is, perhaps, less evident to a parent or teacher, but it is highly intrusive and the hurt it causes can be very severe.
Incidents of known or suspected cases should be reported to the principal and where appropriate the police.
This policy will be reviewed and updated as required i.e. due to new information.