ICT / E-Safety Policy

All staff and students of International Language College using the computing facilities at this school agree to abide by these policy guidelines.

These policy guidelines have been developed to ensure an environment where all students and staff are protected from exposure to illegal, offensive or otherwise inappropriate material or content in an online context.

Electronic/Digital Media

Electronic/digital media cannot be used for knowingly viewing, transmitting, retrieving, or storing anything that is:

1. Discriminatory or harassing
2. Derogatory to any individual or group
3. Obscene, sexually explicit or pornographic
4. Defamatory or threatening
- In violation of any license governing the use of software

6. Engaged in any purpose that is illegal or contrary to the school policy or interests or reputation.

The computers, electronic media and services provided by the school are for educational use to assist staff in the performance of their job.

Limited, occasional, or incidental use of electronic media for personal purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the system's use for their educational purposes and outside school contact hours.

The school expects all staff and students to abide by the principles outlined above when using any of the ILC's ICT equipment. We believe that the dignity of all students and staff must be respected, and that staff and students should be courteous and considerate toward everyone. All those working or studying here have a responsibility to establish and maintain an online environment free from any form of bullying or harassment.

If you break any of the outlined rules you may be expelled from the school with no refund.

Managing ILC's Network

- Firewalls in place on the school's networks will help prevent exposure to harmful materials.
- AVAST! antivirus on all computers prevents access that is potentially threatening to the security of the school's systems 2 ICT & E Safety Policy – Subscription Updated 28/06/2022
- Storage of all data within the school conforms to UK Data Protection requirements.
- Students do not have access to the network containing any confidential information.

- Passwords are in place on all computers and students only have access to the passwords for the student room.
- The WIFI is password protected.
- Data is backed up on a regular basis in case the system needs to be restored.
- Classroom computers are to be locked by the teacher when leaving the classroom to prevent unauthorised access by students.
- Any device loaned by the school to an employee must be used solely to help them in their work.
- The hardware is maintained to ensure there is no health and safety risk.
- Access to the school's network resources from remote locations is restricted and only approved in rare circumstances for purely work related matters.
- No outside agencies, except our IT management organisation, are allowed to access the ILC network.

Mobiles

- In class time student mobile phones and devices should only be used for learning purposes if requested by the teacher. They should be in airplane mode or silent at all other times.
- Personally owned mobile phones and devices brought into school are the responsibility of the device owner. The school accepts no responsibility for their loss, theft or damage.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside a professional capacity.
- Teachers are permitted to use their own mobile phones or devices in a teaching context, such as checking things on the internet for a class, but they must not disclose their personal number, email etc to the students.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- During work time mobile phones and personally-owned devices will be switched off or on 'silent mode' except where needed for work purposes.
- Staff should never use their own photographic equipment (including mobile phones) to take images of students without their explicit and clear consent. If they plan to film or take photos of any under 18s on school equipment, they need to make sure that the student is happy for them to do so and check with the office that the parents have given their consent. Any images should be deleted immediately after use.

Responsibilities

The School Director

- has overall responsibility for ICT and e-safety, including the updating of firewalls and antivirus software.

The Assistant School Director and Designated Safeguarding Lead

- to investigate and record all reported incidents of a breach of this policy.
- to make recommendations to the School Director based on their findings.
- to notify the Designated Safeguarding Lead if any incident involved an Under 18 student
- to follow up on any incident involving an Under 18.
- to liaise with agents/leaders/families of any Under 18 involved.
- to notify the appropriate authorities if the incident is potentially criminal.

Staff

- to read, understand and help promote the school's e-safety policy and guidance.
- to be aware of e-safety issues related to the use of mobile phones and other devices and monitor their use in classes and as far as is possible outside classes on activities etc.
- to report any suspected misuse, abuse or access to inappropriate materials to the Assistant School Director.
- to model safe, responsible and professional behaviour in their own use of technology
- to ensure any digital communications with students should be on a professional level and only through school based systems, never through personal email, texts etc

Students

- to understand the importance of reporting abuse, misuse or access to inappropriate.
- to know and understand that cyber bullying will not be tolerated.
- to understand the importance of adopting good e-safety practice, particularly in relation to under 18s Homestays.
- to understand the importance of adopting good e-safety practice in their own homes, especially when hosting under 18s.
- to report any suspected misuse, abuse or access to inappropriate materials to the accommodation manager, who will report it to the Vice Principal.

Key People

Tony Martin – School Director

Sarah Lally – Assistant School Director / Designated Safeguarding Lead

Mabel Arguelles – Designated Safeguarding Lead

Current Technology

PC/Desktops

Wifi

Smart TV