The English Language Centre
BRIGHTON / CHESTER / EASTBOURNE

ELC Brighton
33 Palmeira Mansions
Brighton & Hove BN3 2GB

info@elc-brighton.co.uk
+44 1273 721771
www.elc-schools.com

ELC Chester
9-11 Stanley Place
Chester CH1 2LU

info@elc-chester.co.uk
+44 1244 318913
www.elc-schools.com

ELC Eastbourne
8 Trinity Trees
Eastbourne BN21 3LD

info@elc-eastbourne.co.uk
+44 1323 639271
www.elc-schools.com

Information and Communications Technology (ICT) Policy and Procedures

1. The purpose of this policy is to:

- set out the key principles expected of all members of the school community at ELC with respect to the use of ICT-based technologies.
- safeguard and protect the children, students and staff of ELC schools
- assist school staff working with students to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

2. The main areas of risk for our school community can be summarised as follows:

- exposure to or sharing of inappropriate content, including online pornography, ignoring age ratings in games, exposure to violence associated with often racist language, substance abuse.
- lifestyle websites and apps, for example pro-anorexia/self-harm/suicide sites.
- hate sites, including extremist websites that encourage radicalisation covered in the school’s Prevent Policy
- grooming and sexploitation
- cyber-bullying in all forms, in particular through social media sites probably accessed through smart phones
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

3. Responsibilities of Key Personnel

CEO	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security with the Group Finance Manager • To ensure the school uses an approved, filtered Internet Service
Centre Manager (Designated Safeguarding	• To promote an awareness and commitment to e-safeguarding throughout the school community

Lead)

- To ensure all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- To ensure that a safeguarding record is made in case of an incident involving a student under 18
- Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming or sexploitation
    - cyber-bullying and use of social media
- To oversee the delivery of the e-safety element of induction for under 18s

IT support (SEBS)

- To report any e-Safety related issues that arise to the CEO/Designated Safeguarding Lead.
- To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed
- To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date)
- To ensure the security of the school ICT system
- The school's policy on web filtering is applied and updated on a regular basis
- That the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the CEO for investigation
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Teachers

- To supervise and guide students under 18 carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)

All staff

- To read, understand and help promote the school's e-safety guidance as set out in this policy.
- Not to access inappropriate material online while at work. This may amount to gross misconduct and summary dismissal.
- To 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
- To report any suspected misuse or problem to the Designated Safeguarding Lead
- To model safe, responsible and professional behaviours in their own use of technology
- To ensure that any digital communications with students and ex-students should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Students

- to understand the importance of reporting abuse, misuse or access to inappropriate materials, particularly in relation to students under the age of 18

- To know and understand school policy on the taking / use of images and on cyber-bullying.
- To understand the importance of adopting good e-safety practice when using digital technologies particularly in relation to students under the age of 18

Homestays

- to understand the importance of reporting abuse, misuse or access to inappropriate materials, particularly in relation to students under the age of 18

4. Communication:

- Policy to be posted on the school website and link in the Staff Guide
- All students under 16 and closed groups under 18 to have an IT safe use induction as part of their school induction
- Staff and homestay responsibilities summarised in staff code of conduct for under 18 year olds

5. e-Safety and students

While access to the internet and phones are wonderful ways for people to stay in touch with their friends and family, they also provide darker opportunities for abuse and inappropriate behaviour. In particular, there are risks to young people through cyber bullying (possibly by their peers), grooming by adult sexual predators, and illegal downloading of illegal or copyrighted materials and possibly IT viruses. The school has therefore established the following guidelines:

1) Staff should not give out their personal mobile number, email address, Facebook or social media contact details to students, especially those under 18. The exception to this would be homestays providing emergency contact details to a young student.
2) Inappropriate access to websites should be reported to the Centre Manager. Inappropriate websites include pornographic sites, excessively violent videos and games, and some age inappropriate social networks and chat rooms. Most inappropriate sites are in fact blocked on the school network, but may be accessed by students in a home setting. Therefore, all staff are asked to be vigilant regarding use of the internet by under 18 year olds, and if there are concerns about content, excessive use or possible grooming or abuse, they should be reported and/or action taken to remove access. Staff are also not expected to access these sites (see staff responsibilities above).
3) Where possible, in a homestay access to Wi-Fi should be restricted, particularly after bedtime, to ensure that young students are not distracted and get enough sleep.
4) Notices about staying safe online are displayed in the school and in particular in the computer rooms. Groups of younger learners, for example under-16s and closed groups under 18, will have a special session as part of their induction on e-safety. In particular, students will
    - understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - understand why on-line ‘friends’ may not be who they say they are and to understand why they should be careful in online environments;

- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- understand why they must not post pictures or videos of others without their permission;
- know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies

6. Managing the ICT infrastructure

6.1 Internet access, security (virus protection) and filtering

The school:

- Uses a filtering system on the student network which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, extremism etc.
- Ensures network is healthy through use of anti-virus software and a firewall
- Blocks all Chat rooms except those that are part of an educational network or approved Learning Platform;
- Is vigilant in its supervision of children's use at all times, as far as is reasonable;
- Is vigilant when conducting 'raw' image search with children e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Principal;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme (see separate appendix);
- Provides advice and information on reporting offensive materials, abuse/ bullying etc

6.2 Network management (user access, backup)

This school:

- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- Makes clear that no one should log on as another user
- Requires all users to always log off when they have finished working
- Makes clear that staff are responsible for ensuring that any computer, tablet or laptop loaned to them by the school, is used solely to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data;
- Our wireless network has been secured to appropriate standards suitable for educational use;

- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

6.3 Passwords policy

- All admin staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private and to change it when required.

7. School website

- Any photographs published on the web are published with the written approval of the people in them and do not have full names attached;
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using school approved blogs or wikis to password protect them.

8. Personal mobile phones and mobile devices

- Student mobile phones and personally-owned devices should only be used for learning purposes in class time. They should be in airplane mode or silent at other times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Personal devices used in the school should be maintained to safety requirements - this is the responsibility of the user. Unsafe equipment should not be used on the school premises.

9. Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a private capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- 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.

10. Personal Use of Systems

The school permits the incidental personal use of school IT and other equipment provided that:

- use must be minimal and take place substantially out of normal working hours (that is, during a usual lunch hour, before or after standard work hours);
- all personal e-mails are labelled "Personal" in the subject header;
- It does not interfere in any way with the User carrying out his duties on behalf of the school;
- it does not commit the school to any marginal costs; and

- it complies with the school's policies including this policy.

The policy to allow continued personal use is dependent upon its not being abused and the school reserves the right to withdraw permission from any User, group of Users or all Users or to amend the scope of this policy at any time and at its absolute discretion.

Misuse or abuse of school equipment in breach of this policy will be dealt with in accordance with our disciplinary procedure. Serious breaches may amount to gross misconduct which can lead to summary dismissal. Misuse can, in certain circumstances, constitute a criminal offence and may result in a report to the police.

When opening email from external sources users must exercise caution in light of the risk viruses pose to system security. Users should always ensure that they know what an attachment is before opening it. If a user suspects that their computer has been affected by a virus they must contact the Principal immediately.

No external equipment or device may be connected to or used in conjunction with the school's equipment or systems without the prior express permission of the Principal.

11. Asset disposal

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

12. Links to other Policies and documents:

ELC Disciplinary Policy and Procedure
ELC Safeguarding and Child Protection Policy
ELC Policy on Abusive Behaviour
ELC Staff Code of Conduct

Policy reviewed May 2024 by the Senior Management Team
Next review May 2025