LLE Safeguarding Policy (SP)

SP9 – E-Safety Policy

Date of policy: 20 May 2015

Last reviewed: 2 January 2018, 14 December 2018, 4 December 2019, 11 December 2020, 14 January 2022, 20 January 2023; 29 October 2023; 20 December 2024

Next review date: December 2025 or whenever necessary

This policy applies to all members of the LLE community (including staff, students, parents/carers, visitors and guests in the homestay). It is a statement of the aims, principles, strategies and procedures for e-safety throughout LLE. The E-Safety Policy should be read in conjunction with our Data Protection and Information Sharing Policy and Safeguarding Policy.

You have a responsibility to the students in your care to know what they are doing online during their stay with you.

What is E-Safety?

E-Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way, also about supporting children and adults to develop safe online behaviours.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies such as texting and phone calls are also covered by the term 'E-Safety'.

Online Safety

It is essential that children are safeguarded from potentially harmful and inappropriate online material.

The breadth of issues classified within online safety can be categorised into four areas of risk for children, also known as the 4 c's:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group: apwg.org

Use of Mobile phones

LLE is aware that many of our students including children aged under 18 years old will have unlimited and unrestricted access to the internet via their mobile phone networks (i.e. 4G and 5G).

LLE teachers and homestay hosts are expected to monitor students' mobile phone and internet use.

Teachers/homestay hosts should also be aware that students are able to use their mobile phones as a "hot spot" where they are then able to access the internet from other internet enabled devices. This access means some children, whilst at school and despite the school having restricted access to the internet can still sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

LLE is also aware that this could happen in the teacher/homestay host's home, despite the teacher/ homestay host having parental controls on the internet. Any incidences or suspicions should be reported to the Deputy Designated Safeguarding Lead or DSL immediately.

Why provide internet access?

The internet is an essential element in 21st century life for education, business and social interaction. LLE encourages the provision of quality internet access to enhance the learning experience and as a necessary tool for teachers to support their professional work through access to online ELT resources.

LLE teachers are expected to install appropriate parental control software on their routers.

Parental controls however cannot block all inappropriate content on-line. A young person who is actively seeking inappropriate content online might be good at disabling or getting around blocking filters and hiding their search history.

We recommend turning off access to the internet during the night where student's internet usage cannot be monitored.

Homestay hosts should be aware of the content of the computer games students are playing, e.g. violence, gambling, sex, drugs, swearing. Please refer to the PEGi rating. If in doubt please check with the Course Managers.

Children can be exposed to biased and extreme opinions on-line for example, eating disorder websites which glorify Anorexia, self-harm sites etc. We need to teach the children in our care how to evaluate what they read and see online and empower children to make safe and informed decisions. Children should be reminded that not everything they read on-line represents the truth.

Internet

- Young Learners should be guided as to what internet use is acceptable and what is not. They will be given clear objectives for internet use in lesson time.
- Young Learners must have adult supervision whilst using the internet.
- LLE teachers should guide students in online activities that will support the learning outcomes planned for the student's age and maturity.
- Internet access will be planned to enrich and extend learning activities.
- Young Learners will be encouraged to tell their teacher immediately if they encounter any material that makes them feel uncomfortable.
- Young Learners will be taught to question information available online before accepting it as true.
- Internet access will be filtered appropriate to the age of the students.

- Access to the internet should be restricted at night time either by removing devices or by turning off the WI-FI.

LLE teachers will ensure that use of internet derived materials complies with copyright law.

Email

- All emails sent must be professional in tone and content.
- Young Learners must immediately tell a teacher if they receive offensive email.
- Young Learners must not reveal personal details of themselves or others in email communication (such as address or telephone number). Young Learners must not arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised by an LLE teacher before sending.
- Young Learners should be made aware that the writer of an email (or the author of a web page) may not be the person claimed.

Social Networking

- All staff, teachers and homestay hosts must not accept friend requests from students or parents on social media accounts or interact with any students or parents via any form of social media.
- Staff, teachers and homestay hosts must not post photos of LLE students aged under 18 on their personal social media accounts.

LLE teachers shall:

- Behave responsibly and professionally at all times in connection with the use of social networking sites and keep up to date with privacy policies of the sites they use.
- Ensure that all communication with Young Learners takes place within clear and explicit professional boundaries.
- Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Deputy Safeguarding Lead if they are unsure.
- Co-operate with LLE in ensuring the implementation of this policy.

Chatrooms and Instant Messaging

Young Learners are not permitted to use these facilities on a teacher's computer whilst on a LLE course.

Video Conferencing and other Video Communications

- Young Learners will not be allowed unsupervised access to video communications.
- Digital communication between LLE and students or parents/carers must be professional in tone and content.

LLE Students (Young Learners):

- Must hand mobile phones, tablets, portable electronic games and media players brought to the course by Young Learners to the teacher at night-time, if requested by the teacher.
- Are forbidden from sending abusive or inappropriate text messages
- May have their internet activity checked

LLE Teachers:

- Are allowed to take digital photographs and video images to support educational aims, but must follow guidance in the LLE Photography Policy concerning the taking, sharing, distribution and publication of those images.

LLE Website

- The point of contact on the website will be the school address, email and telephone number. Teacher or student personal information will not be published.
- Website photographs that include young learners will be selected carefully and will only be published with parental permission.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.

Cyberbullying

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When children are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety. Cyberbullying (along with all forms of bullying) will not be tolerated. All incidents reported will be recorded and investigated. Please refer to SP8: LLE Bullying Policy and Procedure.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet.

Keeping Children Safe in Education 2022 defines cyber crime as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

- Unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;
- Denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- Making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may accidentally or deliberately stray into cyber-dependent crime. Any incidences or suspected incidences of cyber crime should be reported straight away to the Designated Safeguarding Leads, who would take the appropriate further action with the police.

If there are concerns about a child in this area, the designated safeguarding leads will also consider referring the child into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

LLE Teacher ICT and Data Security

- LLE teachers must not share their user account details and must not leave their computers unlocked and accessible to students.
- In lessons where internet use is pre-planned, Young Learners are guided to sites **checked as suitable** for their use beforehand.
- Where Young Learners are allowed to freely search the internet, eg: using search engines, teachers are vigilant in monitoring the content of the websites the young people visit and encourage Young Learners to use specific search terms to reduce the likelihood of coming across unsuitable material.

Young Learners

- All Young Learners must sign the LLE Student Code of Conduct for Young Learners (on the LLE Safeguarding form).
- E-Safety rules will be given to Young Learners in their student handbook and will be discussed with students at the start of the course.
- Any breaches of the Student Code of Conduct with reference to ICT for Young Learners will be referred directly to LLE and Internet access will be denied.
- Young Learners will be informed that network and internet use on a teacher's computer will be monitored.
- Students' work will only be published with the permission of the student (and parents in the case of Young Learners).

Parental Support

- Parents' attention will be drawn to LLE's E-Safety Policy in the pre-course information (student handbook)
- Parents will be asked to read through the LLE Student Code of Conduct with their child on the LLE Safeguarding Form for Young Learners and for the student to sign the agreement.

Policy Implementation

All new LLE teachers receive e-safety advice and guidance as part of their induction programme to ensure they understand their responsibilities, as detailed in this policy.

Further Information

If you would like free independent advice and support about keeping children safe online than you can call the free **NSPCC Online Safety Helpline: 0808 800 5002**.
https://www.nspcc.org.uk/keeping-children-safe/reporting-abuse/nspcc-helpline/

For further details on setting parental controls on your home WI-FI connections then please contact your internet provider.

Further information on Social Media sites can also be found here: https://www.nspcc.org.uk/keeping-children-safe/online-safety/