ONLINE SAFETY (E-SAFETY) policy 2020/2021

Aim:

- To educate all students about being safe on-line.
- To provide an environment in which students are protected from exposure to illegal, offensive or otherwise inappropriate material online.
- To ensure the security of LanguageUK computer and network systems.
- To develop a policy that will not adversely affect the learning experience.

This policy is applicable to all staff management, teaching, and administrative – and students 18 years old and over as well as U18's. It applies to staff and students always and in all areas of LanguageUK including the main college site where business is undertaken.

In all cases, this policy resolves, as far as possible, to prevent students being exposed to harmful material; prevent students being subject to harmful online interaction with other users (grooming, indoctrination, radicalisation etc.); and prevent students using the internet in a way that is potentially harmful to themselves and / or others.

Internet Access:

- LanguageUK is wireless enabled, and every classroom and office has at least one computer with internet access. LanguageUK staff may use the school's computer systems in the conduct of their duties, including lesson preparation, ensuring that any material accessed is appropriate for use with their class, considering the age and cultural sensitivities of the students.
- Students may use their own devices to access other websites to assist them in their studies.
- However, staff and students are strictly forbidden to access, either on the school system or their own 4G or 5G networks, any site which is deemed inappropriate, in line with the government's Prevent policy.
- Unless it is for a class activity, work assignments, student presentation under the guidance and monitoring by a teacher, students are not allowed to use the computer in the classroom. LanguageUK has a dedicated computer lab for the students. Access to Admin office computer by a student is strictly forbidden.
- Firewalls are in place on the LanguageUK own networks, but all staff must be aware that students will have their own 4G/5G networks roaming which may not have the same protection. Whilst LanguageUK accept that it is impossible to control what a device with a 4G/5G network can access, it is nonetheless the responsibility off all staff to be alert and ensure, as far as humanly possible, that students do not access any websites which may be prohibited by this policy. The firewalls in place on LanguageUK networks prevent the user accessing websites in the following categories, on the grounds that they are illegal, potentially illegal, inappropriate, offensive, or potentially threatening to the security of the school's systems:
- Violence/hate/racism
- Nudism
- Pornography
- Weapons
- Adult/mature content
- Cult/occult
- Drugs/illegal drugs
- Illegal skills/questionable skills
- Gambling
- Games
- Military
- Political/advocacy groups
- Hacking/proxy avoidance systems

- Personals and dating
- Usenet news groups
- Freeware/software downloads
- Pay to surf sites
- Advertisement
- Web hosting
- Malware
- Any other potentially illegal / inappropriate website not covered by the above

Helping under 18 stay safe on-Line:

LanguageUK recognises responsibility to ensure safety of U18s when they are using the internet, social media and other forms of media. Maximum effort is made to guide them in making good choices.

Cyber Bullying:

Cyber Bullying is the misuse of digital technologies or communications to bully a person or a group, typically through messages or actions that are threatening and/or intended to cause offence, anxiety or humiliation. It comes in many different forms and is particularly damaging as the abuse in inescapable - it follows the target everywhere.

Privacy and information sharing:

Most social media sites allow young users to host a public profile, which presents many concerns regarding their privacy. If privacy settings are not applied, the content they publish on their profiles will be accessible to millions of people worldwide.

This information can potentially include:

- Personal contact details.
- Photographs or videos of themselves and their friends.
- The names and addresses of the schools and clubs they attend.
- Their exact locations at any given time using location tagging features.

Digital footprints:

Due to the lack of face-to-face communication in cyberspace, there is a tendency for the offline world to be referred to as the 'real world'. This can be a damaging notion, as it often leads children to act with less caution when using the internet. Behaviour can include:

- Involvement in visible, public arguments.
- The expressing of opinions that can be interpreted as offensive or aggressive.
- Participation in bullying through commenting on or sharing malicious content.

The internet is like a giant USB that saves all the things that we publish online. The collective history of this activity is often referred to as a digital footprint and can be accessed by anyone through a simple online search. If a child or adult uses privacy settings on social media platforms, they will not be able to stop their connections from passing the content they post on to others.

If the activity is offensive, they may find themselves in trouble with peers, the school or even the police. Universities and employers have been known to check the online profiles of applications, so negative activity can also affect a young person's educational and professional opportunities later in life. It is therefore extremely important that young people understand that the cyber world is the real world, with very real consequences.

Grooming and sexual abuse:

Online grooming is the action of an adult befriending a U18 with the intent to prepare them for sexual abuse. It is not a one-off event but a process of engaging with them, tapping into their hobbies and vulnerabilities and building a falsely perceived connection.

Social media, interactive gaming and chat rooms can be the first point of contact. Abusers can hide behind false online identities and talk to young people with greater ease, out of the direct observation of others.

If a student U18 has been receiving inappropriate communications from an adult, LanguageUK will report this on https://www.saferinternet.org.uk/advice-centre/need-help

Exposure to pornographic or violent material:

Inappropriate content doesn't have to be intentionally sourced. Often U18 will stumble across it by chance; disguised under seemingly innocent attachments, or even circulated on leading social media sites. The most concerning material includes:

- Extreme or abusive pornography.
- Excessive violence or explicit physical attacks.
- Hateful material expressing racist, sexist, homophobic or transphobic opinion.
- Harmful advice encouraging eating disorders, self-harm or suicide.

Sexualisation:

Young people, most commonly girls, often feel under pressure to act provocatively or be perceived in a sexual way. This pressure can come directly from peers or partners, or indirectly through the commercialisation of sex in mainstream media and marketing industries. When using the internet, this can motivate young people to:

- Post provocative images of themselves on social media.
- Perform sexual acts over webcam, send sexually explicit photographs to another person or pressurize others into doing so.
- Search for pornographic images and videos.

LanguageUK Internet safety tips:

- Never give out your real name.
- Never tell anyone where you go to school.
- Only meet someone from a chatroom in a public place with one of your parents or another adult. If they are genuinely who they say they are they will be happy to do this.
- Never give out your address or telephone number.
- Never agree to meet anyone from a chatroom on your own.
- Tell an adult if someone makes inappropriate suggestions to you or makes you feel uncomfortable online.

Policy issued Oct 2016
Review date October 2017
Reviewed Sept 2017
Reviewed October 2018
Reviewed October 2019
Reviewed October 2020
Next review October 2021