LANGUAGEUK ONLINE SAFETY POLICY

Designated Specialist Safeguarding Lead (DSL) team Level 3	Prof.Ece Inan Chris Hopson- ADos
Designated Advanced Safeguarding Person (DSP) team Level 2	Kasia Malkowaska DoS
Online-safety lead	Prof.Ece Inan
Date this policy was reviewed and by whom	1st November 2023 E.Inan-DSL
Date of next review and by whom	On-going E.Inan Reviewed November 2023 Will be reviewed November 2024

This Policy aims to:

- Set out expectations for all LanguageUK staff and teaching members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all staff and teachers to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of LanguageUK school, and regardless of device or platform
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of LanguageUK supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Roles and Responsibilities

LanguageUK staff and teachers have a duty to behave respectfully online and offline, to use technology for teaching and learning, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families, and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Liaise with the designated safeguarding lead on all online safety issues that might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practices in information handling; work with the DSL to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support carefully and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.

Designated specialist Lead Safeguarding Lead/Online Safeguarding lead

Key responsibilities (remember the DSL can delegate certain online safety duties, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2019):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure "An effective approach to online safety, to protect and educate the whole school in their use of technology and establishes procedures to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority https://www.kscmp.org.uk/and work with other agencies in line with Working Together to Safeguard Children".
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Work with the Vice Principal to ensure a GDPR-compliant framework for storing data while helping to ensure that child protection is always put first, and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safety.
- Review and update this policy, other online safety documents (e.g., Acceptable Use Policies), and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent, and others).
- Receive regular updates in online safety issues and legislation.

- Ensure that online safety education is embedded across the timetable.
- Promote an awareness and commitment to online safety throughout.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Facilitate training and advice for all staff.

All Staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are Verity Sessions and Kasia Malkowska.
- Read and follow this policy in conjunction with the school's main safeguarding policy.
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff acceptable use policy and code of conduct.
- Notify the DSL if the policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon.
- Prepare and check all online sources and resources before using within the classroom.
- Notify the DSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual.
- Be aware that you are often most likely to see or overhear online safety issues. Receive regular updates from the DSL and have a healthy curiosity for online safety issues.

Model safe, responsible, and professional behaviours in their own use of technology.

This includes outside the working and teaching hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers, and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.

- **Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local news please note all students are asked to sign on the application form or consent form for U18.**
- Staff can take digital/video images to support educational aims, but must follow LanguageUK policies concerning the sharing, distribution, and publication of those

images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish, or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents or carers.

Data Protection

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if gaining consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

LanguageUK works together to ensure a GDPR-compliant framework for storing data, which ensures that child protection is always put first, and data-protection processes support careful and legal sharing of information.
Staff are reminded that all safeguarding data is highly sensitive and should always be treated with the strictest confidentiality, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Students

Key responsibilities:

- Understand the importance of reporting abuse, misuse, or access to inappropriate materials.
- Read and sign the section for students in the parental consent form.
- Read and sign the code of conduct for adults or U18.

- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technology.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems. **Parents and Carers Key responsibilities:**
- Read, and sign the parental consent form
- Consult with LanguageUK if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and model safe, responsible, and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening, or violent comments about others.

Staff guidance on how to maintain well-being and safety online:
There is strong evidence that indicates that feeling close to, and valued by, other people is a fundamental human need and one that contributes to functioning well in the world.
https://www.mind.org.uk/workplace/mental-health-at-work/taking-care-of-yourself/five-ways-towellbeing/
https://www.internationalsos.com/client-magazines/maintaining-your-mental-wellbeing-whileworking-from-home
https://www.marshcommercial.co.uk/articles/maintain-your-mental-wellbeing-during-quarantine/
If any staff require extra information, please email verity@languageuk.com

Handling online safety concerns and incidents
It is vital that all staff recognise that online safety is a part of General concerns and must be handled in the same way as any other safeguarding concern.
Safeguarding is often referred to as a jigsaw puzzle, so all staff should err on the side of talking to the online safety lead / Designated Safeguarding Lead (DSL) to contribute to the overall picture or highlight what might not yet be a problem.
School procedures for dealing with online safety will be detailed in the following policies:
- LanguageUK Safeguarding and Adults at Risk Policy
- Anti-Bullying Policy
- Prevent Risk Assessment
- Data Protection Policy, agreements, and other documentation (e.g., privacy statement and consent forms for data sharing, image use etc.)

You can find all our policies either online on the website or in the administration office and Staff room at the school.

- Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.
- Any concern/allegation about staff misuse is always referred directly to the Safeguarding Officer Staff may also use the **NSPCC Whistleblowing Helpline**. **0808 800 5000 or emailing help@NSPCC.org.uk**

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 the Admin office computer by a student is strictly forbidden.
- Firewalls are in place on 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 accepts that it is impossible to control what a device with a 4G/5G network can access, it is nonetheless the responsibility of all staff to be alert and ensure, as far as humanly possible, that students do not access any websites that may be prohibited by this policy. The firewalls in place on LanguageUK networks prevent the user from 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 Online:
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 perceive 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.

The school will actively seek support from other agencies as needed (i.e., the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, Prevent

Officer, Police). We will inform parents/carers of online-safety incidents involving their children, and the Police

where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law. https://www.saferinternet.org.uk/advice-centre/need-help https://report.iwf.org.uk/en/ https://www.gov.uk/report-terrorism https://www.report-it.org.uk/

Policy written 27th May 2020
Reviewed October 2020
Reviewed October 2021
Reviewed September 2022
Revised November 2023