

Department	Language in Action	Implementation Date	15 th May 2026
Official name of the policy	E-Safety and Cyber-Bullying Policy and Procedure (v2.0)	Last Reviewed/Update Date	15 th May 2026
Policy Owner	Adam Ennis (Head of Juniors)	Approval Date	15 th May 2026
Policy Approver	Emiliano Sallustri (Managing Director ELT – Designated Safeguarding Lead)	Next Review	15 th May 2027

E-Safety and Cyber-Bullying Policy and Procedure

1. Introduction and Aims

Language in Action recognises the benefits and opportunities which new technologies offer to teaching and learning and prides itself on its integration of technology into the learning environment.

We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills and to enable our students to achieve their learning goals. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use, including cyber-bullying and harassment.

Central to the company's approach is the belief that all students have a right not to be bullied and that bullying is always unacceptable. Language in Action also recognises that it must take note of bullying perpetrated outside school which spills over into the school environment.

This policy should be read alongside other relevant school policies relating to Safeguarding and Child Protection, Bullying, Welfare and Discipline.

2. Creation, Monitoring and Review

This policy has been created by the DSL in consultation with other stakeholders and its impact is monitored regularly, with a full review being carried out annually. The policy will also be reconsidered where particular concerns are raised or where an e-safety or cyber-bullying incident has been recorded.

3. Policy Scope

The policy applies to all users of Language in Action's IT systems, both on the premises and remotely. It covers all use of the internet and forms of electronic communication such as email, mobile phones, social media sites, chat rooms, and any other electronic means of contact.

Definition of Cyber-Bullying

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend themselves.

By cyber-bullying, we mean bullying by electronic media, including:

- Bullying by texts, messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, including blogs, personal websites and social networking sites
- Using e-mail to harass or threaten others
- Hijacking or cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on any social media platform

Legal Issues

Cyber-bullying is generally criminal in character. The law applies to cyberspace.

- It is unlawful to disseminate defamatory information in any media including internet sites.

- Section 127 of the Communications Act 2003 makes it an offence to send, via a public electronic communications network, a message or other matter that is grossly offensive, indecent, obscene or menacing.
- The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

In line with the approach reflected in the Education and Inspections Act 2006, Language in Action reserves the right to address cyber-bullying, and any bullying aspects, carried out by students on or off site. The Welfare Officer is the first point of contact for such matters at centre level.

Roles and Responsibilities

The primary point of contact for all concerns regarding e-Safety and cyber-bullying is Language in Action's designated Welfare Officer or the Designated Safeguarding Lead (DSL). The DSL takes lead responsibility for online safety, including understanding and overseeing the organisation's filtering and monitoring systems, in line with KCSIE 2025.

All staff are responsible for ensuring the safety of students and colleagues, and should report any concerns immediately to their line manager, the Welfare Officer (in the case of a student under 18), or the DSL or Deputy DSL in case of DSL absence.

Staff are required to inform all IT users of this policy. When informed about an e-safety or cyber-bullying incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it or to those involved.

All members of the school community have a duty to bring to the attention of the Welfare Officer any example of cyber-bullying or harassment that they know about or suspect.

When any incident is reported, Language in Action undertakes to thoroughly investigate it and to review the existing school policies, updating them where required.

Security

Language in Action endeavours to ensure that the school network is safe and secure. Every effort will be made to keep security software up to date.

Appropriate security measures will include the use of enhanced filtering, firewalls, antivirus protection, servers, routers and workstations to prevent accidental or malicious access of school systems and information.

No student is allowed to work on the internet in any location within the school without a member of staff present. Digital communications, including email and internet postings over the school network, will be monitored in line with all Language in Action policies.

Behaviour

Language in Action will ensure that all users of technologies adhere to the standard of behaviour set out in our Behaviour Policy and Terms and Conditions.

The school will not tolerate any abuse of IT systems. Whether offline or online, all communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying, harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Good conduct includes only using mobile telephones and other devices at appropriate times so as not to disrupt the learning of others. Students are asked to switch off mobile devices when in class.

Where conduct is found to be unacceptable the school will deal with the matter internally. Where conduct is considered illegal, the school will escalate the matter through the Group Safeguarding Governance structure, who will report the case to the appropriate authorities.

Language in Action reserves the right to use the full range of sanctions to correct, punish or remove students who bully fellow students or harass staff, both in or out of school. Language in Action will also use its power of confiscation where necessary to prevent students from committing crimes or misusing equipment.

Appropriate Usage for Students Under 18

The majority of students within the school are under 18 and therefore the following measures are in place:

- Students are not allowed to use computers on LiA-rented main premises. In exceptional cases, adult supervision is required to protect children from viewing inappropriate material.

- Careful monitoring to ensure there is no use of phones in class, in accordance with the class rules for all students, including under 18s.
- Informal monitoring during break times or social activities when students are using their own tablets and phones.
- Encouraging teachers, especially those of closed group under 18 classes, to discuss e-safety and cyber-bullying issues in class.

Language in Action educates its students in the proper use of telecommunications and about the serious consequences of cyber-bullying and will continue to inform and educate its students in these fast-changing areas.

Use of Images and Video

The use of images, photographs and video is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person.

Photographs of activities on the main premises should be considered carefully and have the consent of Centre Management staff before being published. Approved photographs should not include names of individuals without prior written consent.

The use of mobile phone cameras to cause distress, fear or humiliation is strictly prohibited and will be treated as a cyber-bullying incident.

Personal Information

Language in Action is committed to keeping the personal information of its staff and students secure.

No personal information can be posted to the school website without the permission of the person(s) affected, unless it is in line with our Data Protection Policy.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected.

Where personal data is no longer required, it must be securely deleted in line with Language in Action's Data Protection Policy.

Incidents and Response

Where an e-safety or cyber-bullying incident is reported to the school, the matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

If a learner wishes to report an incident, they can do so to their teacher, group leader, or the Welfare Officer for students under 18.

Following any incident, the school undertakes to review what has happened and decide on the most appropriate and proportionate course of action.

Guidance for Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol below:

Mobile Phones

- Ask the student to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message or image, including the date, time and names.
- Make a transcript of any spoken message, again recording date, time and names.
- Tell the student to save the message or image.
- Go with the student to see the Welfare Officer, or in their absence, contact your line manager.

Computers

- Ask the student to display on screen the material in question.
- Ask the student to save the material.
- Print off the offending material straight away.
- Make sure you have all pages in the correct order and that there are no omissions.
- Accompany the student, taking the offending material, to see the Welfare Officer.

Normal procedures to interview students and to take statements will then be followed, particularly if a child protection issue is presented.

Guidance for Students

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your teacher, group leader or the Welfare Officer.
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.
- Stay in public areas in chat rooms.

Guidance for Families, Accompanying Adults and Agents

It is vital that all students are aware of the serious consequences of getting involved in anything that might be seen as cyber-bullying.

If a parent or responsible adult believes that a child in their care is the victim of cyber-bullying, they should save the offending material and contact the Welfare Officer as soon as possible.

Further support and guidance may be obtained from:

- www.bullying.co.uk (Family Lives)
- www.anti-bullyingalliance.org.uk (Anti-Bullying Alliance)
- www.childline.org.uk (Childline, 0800 1111)
- www.ceop.police.uk (CEOP — Child Exploitation and Online Protection Command)

Feedback and Further Information

Language in Action welcomes all constructive feedback on this and any other school policy. If you would like further information, please contact the Head of Department at adam.ennis@malvernplc.com.