INCLUSIVE LEARNING SUPPORT (ILS)

ONLINE SAFETY (E-SAFETY) POLICY

Version: 1.0

Organisation: Inclusive Learning Support (ILS)
Registered Office: Aylesham, Kent
Email: Info@ils-kent.co.uk

Approved By: Director
Effective Date: September 2026
Review: Annually
Review Date: September 2027
Status: Approved / Current

1. POLICY STATEMENT

Inclusive Learning Support (ILS) is committed to providing a safe, secure and supportive learning environment for all children, young people, staff, volunteers and families.

As many of our services involve digital technology, remote communication and online resources, ILS recognises its responsibility to protect children and young people from online risks, including cyberbullying, exploitation, inappropriate content, grooming and online abuse.

Online safety forms an integral part of ILS's wider safeguarding responsibilities.

ILS promotes the safe, responsible and appropriate use of technology while recognising that children and young people may experience risks both within and outside of ILS services.

2. PURPOSE

The purpose of this policy is to:

- Promote safe and responsible use of technology.
- Protect children and young people from online harm.
- Provide clear guidance for staff using digital devices and online services.
- Promote professional boundaries when communicating online.
- Support parents and carers in promoting online safety.
- Protect confidential and personal information.
- Promote safe use of artificial intelligence and other emerging technologies.
- Ensure concerns are identified, reported and managed appropriately.
- Support compliance with safeguarding and data protection requirements.

3. SCOPE

This policy applies to:

- Directors.
- Employees.
- Freelance staff and tutors.
- Volunteers.
- Contractors.
- Agency staff.
- Students on placement.
- Children and young people receiving ILS services.
- Parents and carers where online services are provided.

It covers ILS activities involving:

- Mobile phones.
- Laptops and computers.
- Tablets.
- Email.
- Video conferencing.
- Social media.
- Messaging services.
- Online learning platforms.
- Cloud storage.
- Websites.
- Artificial Intelligence (AI) tools used for work purposes.
- Other digital technology used as part of ILS services.

4. LEGAL AND REGULATORY FRAMEWORK

This policy supports ILS's responsibilities under relevant legislation and guidance, including:

- **Keeping Children Safe in Education (KCSIE), as amended and in force from time to time.**
- **UK General Data Protection Regulation (UK GDPR).**
- **Data Protection Act 2018.**
- **Children Act 1989.**
- **Children Act 2004.**
- **Counter-Terrorism and Security Act 2015 and the Prevent Duty.**
- **Online Safety Act 2023.**
- **Equality Act 2010.**

ILS will review relevant legislation and statutory guidance as part of its policy review process.

5. KEY ONLINE RISKS

ILS recognises that children and young people may encounter different types of online risk.

Content

Children and young people may encounter:

- Violent material.
- Hate content.
- Extremist material.
- Pornographic or sexually inappropriate content.
- Self-harm or suicide-related content.
- Misinformation or harmful information.
- Age-inappropriate material.

Contact

Children and young people may experience:

- Grooming.
- Exploitation.
- Online abuse.
- Unwanted contact.
- Coercion.
- Fraud or scams.
- Contact from individuals attempting to cause harm.

Conduct

Risks may include:

- Cyberbullying.
- Sharing inappropriate images.
- Online harassment.
- Hate speech.
- Peer abuse.
- Inappropriate online behaviour.
- Impersonation or misuse of online accounts.

Commerce

Children and young people may be exposed to:

- Online scams.
- Fraud.

- Gambling.
- Inappropriate advertising.
- Financial exploitation.
- Pressure to purchase products or services.

6. RESPONSIBILITIES

Director

The Director is responsible for ensuring that appropriate online safety arrangements are established and maintained.

The Director will ensure that:

- Appropriate online safety arrangements are in place.
- Staff receive appropriate training.
- Relevant policies are reviewed regularly.
- Serious concerns and incidents are appropriately investigated.
- Appropriate resources and systems are available to support online safety.
- Online safety forms part of the organisation's wider safeguarding arrangements.

Designated Safeguarding Lead (DSL)

The DSL will:

- Manage online safeguarding concerns.
- Provide safeguarding advice and support to staff.
- Liaise with parents, carers and external agencies where appropriate.
- Ensure safeguarding concerns are appropriately recorded.
- Support children and young people where online safety concerns arise.
- Ensure online safeguarding concerns are managed in accordance with ILS safeguarding procedures.

Staff

All ILS staff must:

- Use professional judgement when working online.
- Maintain appropriate professional boundaries.
- Follow ILS safeguarding procedures.
- Protect confidential information.
- Report concerns promptly.
- Use approved systems for work-related communication.
- Follow ILS data protection and information-security requirements.
- Complete required online safety training.

7. SAFE USE OF TECHNOLOGY

ILS staff are expected to:

- Use password-protected devices.
- Use multi-factor authentication where available.
- Lock devices when unattended.
- Keep operating systems and software appropriately updated.
- Use appropriate security measures.
- Store personal information securely.
- Use encrypted storage or secure systems where appropriate.
- Avoid accessing confidential information through insecure public networks unless an appropriate secure connection is being used.
- Report suspected loss, theft or compromise of devices or information immediately.

Personal devices must not be used to store confidential ILS records unless this has been expressly authorised and the device is appropriately secured.

8. REMOTE LEARNING AND VIDEO CALLS

When delivering online support:

- Sessions should normally be arranged in advance.
- Parents or carers should be informed where appropriate.
- Staff must maintain professional language and behaviour.
- Appropriate clothing and professional backgrounds should be used.
- Sessions must be delivered using approved platforms where available.
- Staff should take reasonable steps to protect the privacy of children and young people during online sessions.
- Staff must not disclose confidential information unnecessarily during online sessions.
- Online sessions should not be recorded unless there is an appropriate lawful basis, a documented organisational reason and appropriate safeguards.
- Any recording must be handled in accordance with ILS data protection and retention procedures.
- Concerns arising during an online session must be reported in accordance with the ILS Safeguarding & Child Protection Policy.

9. PROFESSIONAL ONLINE COMMUNICATION

ILS staff must communicate with children and families using authorised ILS communication methods.

Staff must not:

- Use personal social media accounts to contact children receiving ILS services.
- Accept personal friend or follow requests from children receiving ILS services.

- Share personal telephone numbers without appropriate authorisation.
- Use personal messaging applications for work-related communication unless expressly authorised under ILS procedures.
- Communicate with children in a manner that could undermine professional boundaries.
- Share confidential information through unauthorised platforms.

All communication with children and young people must be appropriate, professional and safeguarding-focused.

10. SOCIAL MEDIA

ILS encourages responsible and professional use of social media.

Staff must:

- Protect confidential information.
- Maintain professional boundaries.
- Avoid discussing children, young people or families online.
- Avoid sharing confidential organisational information.
- Follow the ILS Staff Code of Conduct.
- Consider the potential impact of online activity on their professional role.
- Report serious or inappropriate online activity relating to ILS where this may create a safeguarding, confidentiality or organisational concern.

ILS staff should not identify children or young people receiving ILS services on personal social media accounts.

11. CYBERBULLYING

ILS takes reports of cyberbullying seriously.

Where cyberbullying involves a child or young person receiving ILS services, the concern will be appropriately recorded and managed in accordance with ILS safeguarding and behaviour procedures.

Where appropriate, ILS may work with:

- Parents and carers.
- Schools or education settings.
- Local authorities.
- Safeguarding professionals.
- Other relevant agencies.

The response will consider the circumstances, seriousness and potential safeguarding impact of the concern.

12. ARTIFICIAL INTELLIGENCE (AI)

ILS recognises that artificial intelligence and emerging technologies can provide useful educational and administrative tools but may also create privacy, safeguarding and accuracy risks.

Where AI tools are used for ILS purposes:

- Personal or confidential information must not be entered into public AI systems unless the use has been appropriately authorised and is compliant with data protection requirements.
- Information relating to children and young people must be handled with particular care.
- AI-generated information must be checked by an appropriately responsible member of staff.
- AI must not replace professional judgement.
- AI must not be used to make significant safeguarding or educational decisions without appropriate human oversight.
- Staff must consider whether AI-generated information is accurate, appropriate and suitable for the intended purpose.
- ILS must consider equality, bias, privacy and safeguarding implications when using AI.

13. DATA PROTECTION

All online information and digital records must be managed in accordance with:

- UK GDPR.
- Data Protection Act 2018.
- ILS GDPR & Data Protection Policy.
- ILS Privacy Notices.
- ILS Confidentiality requirements.
- ILS Data Retention procedures.

Confidential information must only be accessed, stored or shared using approved and appropriately secure systems.

Any suspected or actual personal data breach must be reported immediately in accordance with ILS data breach procedures.

14. REPORTING ONLINE SAFETY CONCERNS

Any online safety or safeguarding concern should be reported promptly to the Designated Safeguarding Lead.

Concerns may include:

- Inappropriate online contact.
- Cyberbullying.
- Grooming.
- Online exploitation.
- Sharing of inappropriate images.
- Online abuse.
- Extremist material.
- Harmful or inappropriate content.
- Serious online harassment.
- Data breaches.
- Unauthorised access to information.
- Loss or theft of devices containing confidential information.

Children, young people, parents, carers, staff and professionals can raise concerns with ILS.

Concerns will be recorded and managed in accordance with ILS safeguarding and data protection procedures.

15. SUPPORT FOR CHILDREN AND YOUNG PEOPLE

ILS aims to help children and young people develop the knowledge and confidence to use technology safely.

Where appropriate, staff may support children and young people to understand:

- Online privacy.
- Safe communication.
- Cyberbullying.
- Grooming and exploitation.
- Appropriate sharing of images and information.
- Online scams and fraud.
- Harmful or inappropriate content.
- Healthy online relationships.
- How and when to report concerns.
- How to seek help from a trusted adult.

Support will be adapted to the child's age, developmental level, communication needs and SEND profile where appropriate.

16. STAFF TRAINING

ILS will provide appropriate training and guidance covering areas such as:

- Online safety.
- Cyber security.
- Data protection.
- Professional boundaries.
- Safe use of digital technology.
- Safe use of AI.
- Recognising online abuse and exploitation.
- Cyberbullying.
- Reporting procedures.
- Safeguarding responsibilities.

Training requirements will be reviewed regularly.

17. MONITORING

ILS may monitor organisational systems, devices and online services where this is necessary and lawful to:

- Protect children and staff.
- Maintain cyber security.
- Prevent misuse.
- Protect confidential information.
- Investigate concerns.
- Meet legal or contractual obligations.

Any monitoring will be proportionate, appropriately authorised and carried out in accordance with applicable data protection requirements.

18. POLICY REVIEW

This policy will be reviewed at least annually, or sooner where necessary.

An earlier review may take place where:

- Legislation changes.
- Statutory guidance changes.
- Significant safeguarding concerns arise.
- Technology or online risks change.
- ILS services or systems change.
- Organisational procedures change.

APPROVAL

Approved by: Neo Matsoso-Ndlovu

Position: Director

Signature: NMN

Date: 09/09/2026

Next Review Date: September 2027

CONTACTING ILS ABOUT ONLINE SAFETY

If you have an online safety or safeguarding concern relating to an ILS service, child or young person, please contact:

Inclusive Learning Support (ILS)
Registered Office: Aylesham, Kent
Email: Info@ils-kent.co.uk

Concerns will be handled in accordance with ILS safeguarding, confidentiality and data protection procedures.