

ONLINE E-SAFETY POLICY

Document Title	Online Safety (E-Safety) Policy
Organisation	Elite Anglo Chinese Services (Company No: 11632695)
Effective Date	27th Sept 2026
Policy Owner	Eve Leung (Deputy Designated Safeguarding & Prevent Lead)
Next Review Date	July 2027 (Subject to required Annual Review)

1. Safeguarding & Emergency Contacts

Role	Name	Contact Details
Designated Safeguarding Lead (DSL)	Evelyn Phillips	Tel: +(044) 01428 648393 Mobile: +(44) 07789 434798 Email: evelyn@eliteacs.com
Designated Deputy Safeguarding Lead (DDSL) and Emergency Contact	Eve Leung	Tel: +(44) 020 88956693 Mobile: +(44) 07787 536030 Email: eve@eliteacs.com / info@eliteacs.com

2. Policy Introduction & Regulatory Framework

The use of the internet and online social networking sites is now an integral part of everyday life for education and social interaction. Students frequently engage with the internet inside and outside of school. However, the increase in use of the internet and social networking sites through mobile devices has raised concerns about online safety, with particular reference to abuse, cyberbullying, grooming, exposure to harmful or age-inappropriate content, and generative AI risks.

This policy forms part of Elite Anglo Chinese Services' (EACS) overall safeguarding arrangements, and all reported online incidents are handled as safeguarding concerns. Good practice in this document aligns with the latest statutory guidance, including Keeping Children Safe in Education and the UK Online Safety Act 2023 and regulatory implementation

2.1 Regular Policy Review & Statutory Governance

Elite Anglo Chinese Services, as a guardianship organisation, keeps its Online Safety Policy under regular review to reflect current UK safeguarding guidance, statutory provisions, and legislative developments relating to children's use of social media and online safety.

2.2 Mandatory Annual Review and Risk Assessment

Technology, and the risks and harms related to it, evolve and change rapidly. Elite Anglo Chinese Services must carry out an annual review of its approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks children in guardianship

face across host families, schools, and online environments.

3. What is Online Abuse?

Online abuse is characterised as abusive behaviour mediated by online platforms, social networks, gaming environments, or mobile technologies. Key forms of online abuse identified include:

- **Cyberbullying:** Abusive comments, rumours, gossip, trolling, and harassment; sharing personal media without consent; or creating malicious sites/profiles.
- **Grooming:** Building emotional connections with a child to gain trust for sexual abuse, exploitation, or radicalisation.
- **Sexual Abuse & Exploitation:** Forcing or persuading a child to take part in sexual activities, including sharing youth-produced sexual imagery.
- **Emotional Abuse:** Ongoing maltreatment online damaging a child's psychological wellbeing.
- **Emerging Risks :** AI-generated harmful media (deepfakes), algorithmically driven self-harm content, and coercive online behaviors on emerging platforms.

4. EACS Procedures for Teaching & Learning E-Safety

- All EACS staff, homestay host families, and drivers must understand the risks posed to children regarding online exposure and abuse.
- The DSL maintains up-to-date training reflecting 2024–2026 UK safeguarding guidance to support the organisation effectively.
- Referral resources include the Child Exploitation and Online Protection (CEOP) center (www.thinkuknow.co.uk).

5. Advice for Students

- Students must adhere to the e-safety policies of their designated school and EACS guidance, both in school and during homestays.
- Students must observe age restrictions on social media and utilize full privacy settings.
- Prohibited activities during homestays include accessing 18+ content (pornographic/gambling sites) or downloading unlicensed files (TV, games, music, PDFs).

6. Advice for Host Families

- **Safe Environment:** Host families must configure safe internet access (firewalls, content filtering, screen-time balance) aligned with NSPCC guidance ([NSPCC Parental Controls](#)).
- **Social Media & Guidance:** Host families should assist students in understanding report/block features, monitoring behavioral changes (e.g., sudden reduction in device use, secretive behavior, distress after phone use, sleep issues).

- Any signs of online harm must immediately be reported to EACS staff.

7. Storage of Information & Data Protection

In accordance with Data Protection legislation and UK GDPR guidelines, all personal data must be stored securely following the EACS Data Protection Policy. Unauthorised cloud storage or removable drives are strictly prohibited.

8. EACS Procedure for Dealing with Online Abuse Reports

- Report Receipt:** Staff receive disclosure or concern via face-to-face, phone, or email.
- Logging:** Details recorded per the Safeguarding & Child Protection Policy and submitted via Safeguarding Referral Form to DSL.
- Emergency Strategy Meeting:** DSL convenes a meeting to assess risk, evaluate vulnerability, and implement a tailored action plan.
- Student Support:** DSL connects student with accredited support (NSPCC, Childline, CEOP) addressing consent, trust, and healthy digital relationships.
- Device Handling & Image Viewing:** Viewing images or seizing devices is strictly restricted to clear safeguarding needs and fully documented. Staff do not search or delete imagery without statutory grounds.
- Statutory Referral:** Immediate referral to Children's Social Care or Police (101/999) if there is risk of harm, adult involvement, coercion, severe exploitation, or imagery involving children under 13.
- Mandatory Deletion Deadlines:** When handling youth-produced imagery safely outside statutory referral, clear deadlines are set for deletion across devices and platforms.

9. Resources & Supporting Guidance

Organisation	Contact / Website	Description
Internet Watch Foundation (IWF)	www.iwf.org.uk	Report illegal child sexual abuse material online.
NCA-CEOP	www.ceopeducation.co.uk/parents www.ceop.police.uk/safety-centre	Safety guidance on gaming, dark web, and reporting grooming or exploitation.
NSPCC Helpline	0808 800 5002 NSPCC	Direct support for adults

Organisation	Contact / Website	Description
	Online Safety Guides	and host families on child online safety.
ChildLine	www.childline.org.uk	Direct support for children and young people.
Professionals Online Safety Helpline (POSH)	0844 381 4772 www.saferinternet.org.uk/about/helpline	Support for safeguarding professionals and educational staff.
Bullying UK / Kidscape	0808 800 2222 www.bullying.co.uk www.kidscape.org.uk	Practical guidance to prevent bullying and cyberbullying.