ELEVATED

A Holistic Approach
To The Education of Young People

E-Safety Policy

1. Statement of Intent

ElevatEd AP Ltd is committed to providing a safe and positive learning environment for all its pupils, both offline and online. We recognise that the internet and digital technologies offer vast educational opportunities, but also present potential risks. This E-Safety Policy outlines our commitment to protecting pupils and staff from online harms, promoting responsible and safe use of technology, and educating our community about digital citizenship.

We understand that pupils attending Alternative Provisions may have particular vulnerabilities or varying levels of digital literacy, and our approach to e-safety is therefore proactive, supportive, and tailored to meet their individual needs.

This policy applies to all users of our digital systems and equipment (including pupils, staff, visitors, and contractors) on and off-site, and covers all digital devices, whether owned by the provision or personal devices used on premises. It will be reviewed annually and updated as necessary to reflect changes in legislation, guidance, and technological advancements.

Signed: Mark Aitken Date: 10.6.25 Review 10.6.26

Mark Aitken

2. Guiding Principles

Our approach to e-safety is guided by the following principles:

- Safeguarding: E-safety is an integral part of our overall safeguarding duties, protecting children from harm and promoting their welfare in the online world.

- Education: Empowering pupils and staff with the knowledge and skills to use technology safely, critically, and responsibly.
- Prevention: Implementing proactive measures, both technical and educational, to minimise exposure to online risks.
- Protection: Providing clear procedures for reporting and responding to e-safety incidents effectively.
- Responsibility: Encouraging all members of our community to take responsibility for their online actions and to report concerns.
- Partnership: Working collaboratively with parents/carers, referring schools, and external agencies to ensure a consistent approach to e-safety.
- Compliance: Adhering to all relevant legislation and statutory guidance, including the Online Safety Act (2023).

3. Roles and Responsibilities

3.1 The Proprietor:

- Ensuring the provision has a comprehensive and effective E-Safety Policy.
- Holding the Head of Provision and E-Safety Lead accountable for its implementation.
- Ensuring adequate resources are allocated for e-safety education, technical infrastructure, and staff training.
- Reviewing e-safety incident reports and ensuring appropriate actions are taken.

3.2 The Head of Provision:

Overall responsibility for the day-to-day implementation and consistent application of this policy.

- Appointing a designated E-Safety Lead and ensuring they have appropriate training and support.
- Ensuring all staff receive regular e-safety training.
- Promoting a culture of online safety across the provision.
- Liaising with parents/carers and external agencies regarding e-safety concerns.

3.3 Designated Safeguarding Lead (DSL):

- The DSL is the primary point of contact for all safeguarding concerns, including those related to e-safety.
- Managing and responding to e-safety incidents that involve safeguarding concerns (e.g., online sexual exploitation, radicalisation, serious cyberbullying).
- Liaising with relevant external agencies (e.g., LADO, police, social care, CEOP).
- Ensuring e-safety is fully integrated into the provision's overall safeguarding procedures.

3.4 E-Safety Lead (or designated staff member):

- Responsible for the day-to-day management of e-safety implementation.

- Advising the Head of Provision and DSL on e-safety matters.
- Overseeing technical e-safety measures (filtering, monitoring).
- Coordinating e-safety education for pupils and staff.
- Acting as a point of contact for e-safety concerns.

Keeping up-to-date with current e-safety threats and guidance.

3.5 All Staff (Teachers, Support Staff, Administration, Volunteers):

- Understanding and adhering to this E-Safety Policy and the Staff Acceptable Use Policy (AUP).
- Modelling safe and responsible online behaviour.
- Integrating e-safety education into the curriculum and daily interactions.
- Being vigilant for e-safety incidents or concerns and reporting them immediately to the E-Safety Lead or DSL.
- Supervising pupils' online activities where appropriate.
- Participating in e-safety training.

3.6 Pupils:

- Understanding and adhering to the Pupil Acceptable Use Policy (AUP).
- Using technology responsibly and respectfully.
- Knowing how to report concerns about online content or contact to a trusted adult.
- Protecting their personal information online.
- Being critical consumers of online information.

3.7 Parents/Carers:

- Supporting the provision's e-safety approach at home.
- Monitoring their child's online activity outside of the provision.
- Discussing online safety with their child.
- Reporting any e-safety concerns to the provision.

4. E-Safety Education

We will provide e-safety education through:

- Curriculum Integration: E-safety topics will be integrated into relevant subjects (e.g. IT/Computing lessons).
- Dedicated Sessions: Regular e-safety lessons, workshops, and awareness campaigns for pupils.
- Discussions: Regular discussions about online risks and responsible use.
- Staff Training: Mandatory annual e-safety training for all staff, covering new threats, guidance, and reporting procedures.
- Parental Engagement: Providing information, resources, and workshops for parents/carers on how to support e-safety at home.

5. Acceptable Use Policy (AUP)

Separate, clear, and age-appropriate Acceptable Use Policies (AUPs) will be in place for:

- Pupils: Detailing expectations for online behaviour, use of provision devices, internet access, social media, and consequences for misuse.
- Staff: Covering professional conduct online, use of provision and personal devices, social media guidelines, and data handling.
- Visitors/Contractors: Briefing on acceptable use of provision Wi-Fi and devices, and safeguarding expectations.
- All users will be required to sign and adhere to the relevant AUP.

6. Managing Online Risks

We employ a multi-layered approach to mitigate online risks:

6.1 Online Content:

- Filtering: Robust internet filtering systems are in place to block access to inappropriate or harmful content. This filtering is regularly reviewed and updated.
- Monitoring: Network monitoring tools are used to identify potential online safety concerns, key word searches, and suspicious activities. Alerts are directed to the E-Safety Lead/DSL.
- Reporting: Clear procedures for pupils and staff to report inappropriate content encountered online.

6.2 Online Contact (Grooming and Exploitation):

- Pupils are educated about the risks of communicating with strangers online and the importance of not sharing personal information.
- Staff are trained to identify signs of online grooming or exploitation and to report concerns immediately to the DSL.
- Where concerns arise, the DSL will follow safeguarding procedures, including referral to the Local Authority Designated Officer (LADO) and/or police (e.g., CEOP).

6.3 Cyberbullying:

- Our Anti-Bullying Policy explicitly covers cyberbullying.
- Pupils are educated on how to prevent, recognise, and report cyberbullying.
- All incidents of cyberbullying will be investigated thoroughly, and appropriate action taken in line with our Behaviour Policy.
- Support will be provided to both victims and perpetrators, using restorative practices where appropriate.

6.4 Online Radicalisation and Extremism (Prevent Duty):

- Staff are trained to recognise the signs of online radicalisation and extremism, in line with the Prevent Duty.
- Filtering systems are designed to block access to extremist content.
- Any concerns about pupils being drawn into terrorism or radicalisation online will be reported to the DSL, who will follow local Prevent referral pathways.

6.5 Privacy and Data Protection:

- Personal data is handled in accordance with our Data Protection Policy and GDPR.
- Pupils are taught the importance of protecting their personal information online.
- Staff are trained on secure data handling practices.

6.6 Gaming and Associated Risks:

- We recognise that online gaming is a popular activity, but it can present risks including:
- Inappropriate Content/Contact: Exposure to offensive language, violent content, or contact with strangers.
- Addiction/Excessive Screen Time: Impact on sleep, education, and physical health.
- In-game Purchases/Gambling-like Mechanics: Financial risks or normalisation of gambling behaviours.
- E-safety education will address these risks, promoting healthy gaming habits and advising pupils to report any uncomfortable online interactions.
- Staff will monitor gaming-related discussions or behaviours for signs of concern.

6.7 Misinformation and Disinformation:

- Pupils will be educated on media literacy, critical thinking skills, and how to evaluate the reliability of online information.

7. Reporting and Responding to E-Safety Incidents

7.1 Reporting Procedures:

- Pupils: Should report any e-safety concerns (e.g., inappropriate content, contact, cyberbullying) to any trusted adult (e.g., teacher, Key Worker, E-Safety Lead, DSL).
- Staff: Must report all e-safety incidents, concerns, or disclosures to the E-Safety Lead or DSL immediately.
- Parents/Carers: Should contact the E-Safety Lead or DSL with any concerns about their child's online safety.

7.2 Incident Response:

- All reported incidents will be logged.
- The E-Safety Lead/DSL will investigate the incident in line with the provision's safeguarding procedures.
- Actions may include:

- Providing immediate support to the pupil(s) involved.
- Liaising with parents/carers and referring schools.
- Disabling user accounts or device access where misuse has occurred.
- Involving external agencies (e.g., police, CEOP, LADO) if the incident meets thresholds for criminal activity or safeguarding concerns.
- Applying appropriate consequences in line with the Behaviour Policy.
- Reviewing and updating relevant policies or procedures.
- Confidentiality will be maintained as far as possible, whilst ensuring the safety and well-being of those involved.

8. Technical Measures

Network Security: Secure networks, firewalls, and antivirus software are in place.

- Device Management: Regular security updates, clear rules for device use, and controlled access to software and apps.
- Wireless Network: Secure Wi-Fi with appropriate access controls.
- Personal Devices: Clear rules will be communicated regarding the use of personal mobile phones and other devices on provision premises (e.g., not allowed during learning time, no photography/recording without consent).

9. Staff Professional Conduct and Use of Technology

- Staff will adhere strictly to the Staff AUP and relevant professional codes of conduct.
- Personal devices should not be used for contact with pupils unless explicitly approved and logged for professional purposes (e.g., emergency calls, official communication platforms).
- Staff will exercise extreme caution regarding their personal social media presence and online interactions to avoid any perception of impropriety or compromising their professional role.

10. Monitoring and Review

- The effectiveness of this policy and our e-safety practices will be monitored through:
- Analysis of reported e-safety incidents.
- Regular reviews of filtering and monitoring logs.
- Feedback from pupils, staff, and parents/carers.
- Keeping up-to-date with new online risks and technologies.
- This policy will be formally reviewed at least annually by the Proprietor and the Head of Provision/Manager.
- Appendix 1: Key External Resources
- NSPCC: Advice and resources on a range of child safety issues, including online safety.
- Thinkuknow (CEOP Education): Online safety education resources for children, young people, parents, and teachers. Report child sexual abuse online.

- Internet Watch Foundation (IWF): Reports and removes child sexual abuse content online.
- UK Safer Internet Centre: Advice, resources, and report harmful content online.
- Parent Zone: Provides information and support to parents on children's digital lives.
- Childline: Offers support and advice for young people.