ONLINE SAFETY POLICY

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027

SAFE PEOPLE • POSITIVE PATHWAYS • COMPLIANT PRACTICE | Impact Alternative Learning - commissioned alternative provision.

1 PROTECTING LEARNERS ONLINE

- Teach safe, respectful and critical online behaviour across lessons, devices, social media, image sharing, gaming and external activities.
- Online harms can occur beyond site; staff treat reports as safeguarding concerns.

2 TECHNICAL FILTERING AND MONITORING

- Identify network/device owner, deploy appropriate filtering and monitoring, assign named review roles and record test/alert responses.
- Review effectiveness at least annually and after incidents/major technology changes; balance protection with reasonable SEND access.

3 STAFF AND LEARNER DEVICES

- Approved use only, with clear rules for photographs, recording, personal devices, Wi-Fi, messaging and public posts.
- No staff-learner personal social media contact; remove access to unsafe content where lawful and safe.

4 ONLINE SEXUAL HARM, GROOMING AND EXPLOITATION

- Escalate coercion, sextortion, non-consensual sharing and child sexual images to DSL promptly; preserve necessary evidence safely without copying/sharing illegal images.
- Follow police/child-protection advice and support affected children sensitively.

5 GENERATIVE AI AND DATA

- Use AI only for authorised educational and admin purposes under adult oversight; verify outputs for bias, inaccuracy and harm.
- Never enter child-identifying, EHCP, medical or safeguarding content into an unapproved AI service.

6 EDUCATION AND PARENTAL PARTNERSHIP

- Teach privacy, digital footprint, exploitation, misinformation, reporting and critical use of AI; offer age- and need-appropriate support.
- Communicate expectations with families and link incidents to safeguarding, data protection and behaviour systems.

ONLINE SAFETY POLICY

Filtering, monitoring, online conduct and generative AI

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027

7 INCIDENT RECORDS AND AUDIT

- Record incident, protective steps, notifications, platform action and follow-up.
- Governance reviews significant online incidents, alerts, training and the technical safeguarding assurance register.

8 DEVICE INCIDENTS AND EVIDENCE MANAGEMENT

- Where online harm is reported, staff do not search personal devices beyond their authority or forward indecent images of children. DSL obtains professional advice and secures devices/data lawfully.
- Use a confidential incident log, consider victim support and police involvement, and avoid making the child repeat traumatic material.

9 FILTERING/MONITORING REVIEW RECORD

- The responsible manager records vendor, product, deployment coverage, safeguarding monitoring roles, test dates, exceptions, alerts and responses.
- Escalate technical failures at once and provide temporary supervision controls until remedied.

10 EXTERNAL WORKSHOPS AND HOME ACCESS

- Review digital risk when learners use third-party Wi-Fi or equipment at music studios, vocational sites, trips and home learning.
- Ensure staff know which organisation owns filtering, evidence and access permissions. Notify commissioner/family of significant risk appropriately.

11 LINKED STATUTORY AND DFE GUIDANCE

- Keeping Children Safe in Education 2026 (in force 1 September 2026); UK GDPR and Data Protection Act 2018 This policy is a provider operational policy; the primary guidance and any commissioner requirements take precedence where applicable.

12 POLICY OWNERSHIP AND REVIEW

- Policy owner: Kate Willis, Principal and Proprietor. Effective date: September 2026. Next review: September 2027, or sooner if legislation, safeguarding guidance, commissioning requirements or provision changes.
- The Principal manages implementation and policy review, with governance oversight where appropriate; relevant staff are informed of updates and confirm understanding.