DATA PROTECTION (GDPR) POLICY

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027

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

1 ACCOUNTABILITY AND RESPONSIBLE PERSONS

- The Principal is responsible for implementation; DPO contact: Kirsty Lampkin. Verify and publish the current DPO contact and controller details before issuing this policy.
- Maintain an information asset register, retention schedule, privacy notices and processor agreements.

2 LAWFUL PROCESSING

- Identify and document a UK GDPR Article 6 lawful basis for each processing purpose and Article 9 condition for special-category data where needed.
- Do not treat consent as the default legal basis for core safeguarding and education processing; record the legal analysis.

3 LEARNER AND EHCP INFORMATION

- Use personal data to provide education, fulfil safeguarding obligations, manage placements, report attendance, support SEN and communicate with commissioners.
- Collect only relevant information; correct errors promptly and restrict staff access to those with a genuine need.

4 SAFEGUARDING DISCLOSURES

- Follow September 2026 DfE information-sharing guidance and applicable legislation; safeguarding can justify prompt lawful disclosure without consent.
- The new section 16LA duty applies only to specified relevant persons. Check Impact's status instead of asserting blanket statutory duty.

5 SECURITY AND AUTHORISED SYSTEMS

- Use approved business accounts, managed permissions, strong passwords, device locking, backup and secure file transfers.
- No personal email, unapproved cloud drives or public generative AI for confidential records; take special care with children's data.

6 DATA SUBJECT RIGHTS

- Log and promptly route data-rights and subject access requests to DPO; verify identity and apply exemptions carefully, especially where another child's privacy or safeguarding may be affected.
- Keep statutory response deadlines under review and record decisions, redactions and correspondence.

DATA PROTECTION (GDPR) POLICY

Lawful, proportionate, secure information handling

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027

7 BREACHES AND ESCALATION

- Staff immediately report wrong-recipient emails, lost devices, inappropriate access or suspected disclosure to the DPO.
- DPO records risk assessment, containment, lessons learned and whether ICO notification (normally within 72 hours once aware, if reportable) or notification to individuals is required.

8 RETENTION, DISPOSAL AND PROCESSOR OVERSIGHT

- Keep records in accordance with an approved schedule and relevant safeguarding requirements, not indefinitely by default.
- Use secure deletion / confidential destruction; complete due diligence and contracts for external processors, including MIS, DBS and cloud services.

9 TRAINING AND AUDIT

- Train staff and contractors at induction and routinely; audit permissions, transfers, retention, breaches and vendor access.
- DPO reports significant risks and overdue actions to Principal and governance.

10 CONTROLLER AND PROCESSOR RESPONSIBILITIES

- Before using third-party platforms, assess whether Impact and commissioner are independent/joint controllers or a processor for the relevant processing; document roles instead of assuming a standard relationship.
- Check contracts, technical security, sub-processors, UK/international transfers and access controls.

11 SAFEGUARDING RECORD SEPARATION AND SARS

- Safeguarding case records require restricted access and contextual handling. In SAR reviews, protect other children, third parties and ongoing child protection work under lawful exemptions.
- A disclosure mistake can have safeguarding consequences: check attachments, recipient identity and redactions before sending.

12 PRIVACY NOTICES, RETENTION AND CCTV

- Provide clear privacy information for learners and carers appropriate to age and accessibility. Define lawful retention, disposal and CCTV use only if CCTV exists in a site.
- Keep accurate records of any surveillance in actual use and maintain a log of access, erasure and rectification requests and decisions.

DATA PROTECTION (GDPR) POLICY

Lawful, proportionate, secure information handling

EFFECTIVE: SEPTEMBER 2026 | REVIEW: SEPTEMBER 2027

13 INCIDENT TABLETOP AND REPORTING

- Practise a data breach scenario involving child records annually with Principal/DPO: containment, recovery, risk, notification, regulatory timetable and safeguards.
- Keep lessons learned and evidence of corrective action, not merely a policy statement.

14 LINKED STATUTORY AND DFE GUIDANCE

- Information sharing to safeguard children and young people (10 September 2026; duty 30 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.

15 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.