ON THE STREETS EDUCATION

Data Protection & E-Safety Policy

1. Policy Statement

The alternative provision is committed to:

- Protecting the **privacy and rights** of students, staff, and stakeholders.
- Ensuring all personal data is handled in compliance with **UK GDPR** and the **Data Protection Act 2018**.
- Maintaining a **safe digital environment** where students can learn and communicate online without risk.
- Embedding e-safety education into all learning programs.

This policy is mandatory for all staff, volunteers, contractors, and students.

2. Scope

This policy applies to:

- **All staff and volunteers**: full-time, part-time, temporary, or contracted.
- **Students and learners**, including offsite or blended provision participants.
- **All data systems**: digital, cloud-based, email, online learning platforms, and paper records.
- **Devices and networks**: laptops, tablets, mobile phones, interactive boards, and IoT devices used in provision.

3. Legal and Regulatory Framework

This policy aligns with:

- **Data Protection Act 2018**
- **UK General Data Protection Regulation (UK GDPR)**
- **Keeping Children Safe in Education (KCSIE) 2025**
- **Children and Families Act 2014 (Special Educational Needs)**
- **Education Act 1996 and 2002** (record-keeping and safeguarding)
- **UK Safer Internet Centre guidance**

Compliance ensures accountability, transparency, and legal protection.

4. Roles & Responsibilities

Role	Responsibilities
Governing Body / Trustees	Approve and review the policy; ensure resources for compliance.
Head of Centre	Oversee implementation, monitor compliance, report breaches.
Data Protection Officer (DPO)	Audit data practices, advise staff, manage breach response, ensure GDPR compliance.
Designated Safeguarding Lead (DSL)	Investigate e-safety incidents with potential safeguarding implications.
Staff	Follow procedures for data handling, reporting, and online safety. Model safe digital behavior.
Students	Adhere to Acceptable Use Policies, report incidents, respect others' privacy online.

5. Data Protection Principles

All personal data must adhere to the **UK GDPR principles**:

1. **Lawfulness, fairness, transparency** – process data only with consent, statutory requirement, or legitimate interest.

2. **Purpose limitation** – collect data strictly for education, safeguarding, or statutory reporting.

3. **Data minimization** – collect only what is necessary.

4. **Accuracy** – maintain up-to-date and correct records.

5. **Storage limitation** – retain only as long as legally required; securely delete afterward.

6. **Integrity and confidentiality** – secure data with encryption, locked cabinets, and role-based access.

6. Data Handling Procedures

6.1 Collection

- Gather only necessary information: personal details, educational needs, medical info, safeguarding concerns.

- Consent forms collected from parents/guardians for under-16s; students over 16 consent where appropriate.

6.2 Storage

- Digital records stored on **encrypted servers** with multi-factor authentication.

- Paper records in **locked cabinets**, access limited to authorised staff.

- Cloud services must comply with GDPR (e.g., Microsoft 365, Google Workspace with educational licenses).

6.3 Access & Confidentiality

- Staff have **role-based access** to data relevant to their duties.
- No sharing of passwords; use secure portals for communication with parents/students.
- Visitors/volunteers sign **confidentiality agreements**.

6.4 Data Retention

Record Type	Retention Period
Student records	Until age 25
Attendance & behaviour logs	7 years
Staff employment records	6 years after leaving
Safeguarding files	Retain per statutory guidance, typically until student reaches 25

6.5 Data Sharing

- Only share data with **statutory agencies**, parents (where appropriate), or partner schools.
- All data-sharing agreements documented.
- Consent required unless legally mandated (e.g., safeguarding concerns).

6.6 Breach Reporting

- All breaches reported to the DPO **within 24 hours**.
- GDPR breach notification to **ICO** within 72 hours if required.

- Internal review conducted to prevent recurrence.

7. E-Safety Policy

7.1 Acceptable Use

- Students and staff must sign **Acceptable Use Agreements**.
- Personal devices may only connect to AP networks with permission.
- Staff model professional use of social media and devices.

7.2 Internet & Device Safety

- Use **firewalls, web filters, and antivirus software**.
- Restrict access to inappropriate content using filtering software.
- Secure Wi-Fi networks with password protection.

7.3 Online Learning & Platforms

- Only use **approved platforms** for remote learning (e.g., Microsoft Teams, Google Classroom).
- Enforce secure login credentials and **two-factor authentication**.
- Monitor student activity to detect misuse or safeguarding risks.

7.4 Cyberbullying & Harassment

- Procedures for students and staff to report online bullying.
- Swift investigation led by DSL or e-safety officer.
- Consequences may include restorative interventions, restricted access, or disciplinary action.

7.5 Social Media

- Staff must not communicate with students via personal accounts.
- Students guided on safe public profiles and digital footprints.
- Use of social media for AP activities must follow a **social media policy** and moderation protocols.

7.6 Staff Training

- Annual e-safety and GDPR refresher courses.
- Updates on new platforms, risks, and safeguarding duties.

8. Safeguarding Integration

- E-safety incidents considered **safeguarding concerns** when appropriate.
- DSL coordinates with local authorities for serious incidents.
- All incidents logged for review and policy improvement.

9. Monitoring and Review

- Continuous monitoring of **network usage, data access, and incident logs**.
- Policy reviewed **annually or after major incidents**.
- Reports to governors include data breaches, e-safety incidents, and compliance audits.

Policy ratified by	**EDAVIES**	**COG**
Review date;	**July 2026**	**Director**