Data Protection Policy/GDPR Policy

Reviewed by:	Richard Fihosy and Claire Ames
Policy Commencement Date:	02.10.2021
Ratified by:	Provision Manager and DSL
Review:	Annual
Next Review:	Autumn Term 2026
Review Date 08.03.24 Richard Fihosy	Page and Sections Page 1 - Former Director's name was deleted.
Aug 25	Full Policy Review

Policy Overview

- This is the official **Data Protection Policy** of AS2Educate.
- We are committed to processing Personal Information fairly, lawfully, and transparently in accordance with the UK GDPR, the Data Protection Act 2018, and subsequent guidance and amendments (e.g. ICO's draft Age-Appropriate Design Code, DfE requirements).
- Processing is necessary to support our provision's operation: staff management, educational delivery, safeguarding, and partnership with children, families, and stakeholders.
- A strong culture of data protection is vital — we treat confidentiality carefully, especially for individuals who may have experienced trauma, understanding that data misuse can retraumatise or harm.

Policy Scope

- This policy, along with related documents (privacy notices, data sharing agreements), sets out how we comply with applicable data protection laws.
- It is mandatory for all staff and the Director Richard Fihosy to adhere to its principles and procedures.
- This policy is not contractual and may be updated at any time to reflect legislative changes or best practice.

Key Definitions

- **Data Subject**: Any identified or identifiable person whose data is held (e.g., staff, pupils, parents).
- **Personal Information**: Includes attendance, medical needs, SEN status, performance, and any recorded images or videos.
- **Special Category Data**: Sensitive data such as health, ethnicity, religion, sexual orientation, and trauma-related disclosures—requires higher protection under law.
- **Data Controller**: AS2Educate determines why and how personal data is processed.
- **Data Users**: Staff and individuals accessing personal data must safeguard it per policy.
- **Processing**: Refers to collection, storage, use, retrieval, sharing, or deletion of personal data.

Data Protection Principles

We commit to upholding the following principles under UK GDPR:

1. Lawfulness, Fairness, and Transparency
2. Purpose Limitation
3. Data Minimisation
4. Accuracy
5. Storage Limitation
6. Security (Integrity & Confidentiality)
7. Accountability — we must demonstrate our compliance (e.g., through records, training, processes).

Data Protection Officer

- **Richard Fihosy** acts as our **DPO**.
- Responsibilities include staff training, conducting audits, advising on data weight matters (e.g. DPIAs), responding to data subject queries, and liaising with the ICO.

Lawful Basis for Processing

We process data only when having one or more lawful bases:

- Consent from the data subject
- Contractual obligation
- Legal obligation
- Vital interests (e.g. emergency medical situations)
- Public task or official function

Special category data is processed only under additional conditions and with proper safeguards.

Consent and Withdrawals

- Consent is explicitly recorded, freely given, informed, and via affirmative action (no pre-ticked boxes).
- Consent is always withdrawable, and we ensure those withdrawing consent clearly understand its effect.

Transparency & Privacy Notices

- We provide clear, accessible Privacy Notices to all data subjects explaining what data we collect, why, and how it is used.
- Notices help build trust, especially with trauma-affected individuals.

Data Minimisation & Accuracy

- Only essential information is collected and processed.
- Individuals can request correction or deletion to ensure records remain accurate and current.

Data Retention and Destruction

- Personal data is retained only for as long as necessary, in line with legal and operational requirements (e.g. safeguarding records, audit evidence).
- Removal and destruction are carried out securely and documented via our internal Records Retention Schedule.

Individual Rights

Data subjects have rights to:

1. Access their data
2. Rectify inaccuracies
3. Request deletion ('right to be forgotten')
4. Restrict processing
5. Object to processing
6. Receive data in a portable format

A clear procedure enables prompt handling of these requests.

Data Security & Trauma-Informed Practice

- Technical (encryption, secure servers) and organisational safeguards are applied to prevent data breaches.
- Staff are trained to handle traumatic disclosures with sensitivity, ensuring confidentiality and care.
- We limit access to special category data to those who need it and use secure, password-protected systems.

Privacy by Design & DPIAs

- New systems or data uses undergo **Data Protection Impact Assessments** (DPIAs) to identify and mitigate privacy risks early.
- Privacy-by-design is integrated into our processes, apps, and infrastructure from the start.

Accountability Measures

We demonstrate compliance via:

- Knowledgeable DPO oversight
- Documented processes and procedures
- Regular internal audits
- Completion of DPIAs
- Staff training and annual refreshers
- Privacy notices and data sharing agreements

Data Sharing

We disclose personal information only when legally justified and appropriately documented. Typical recipients include:

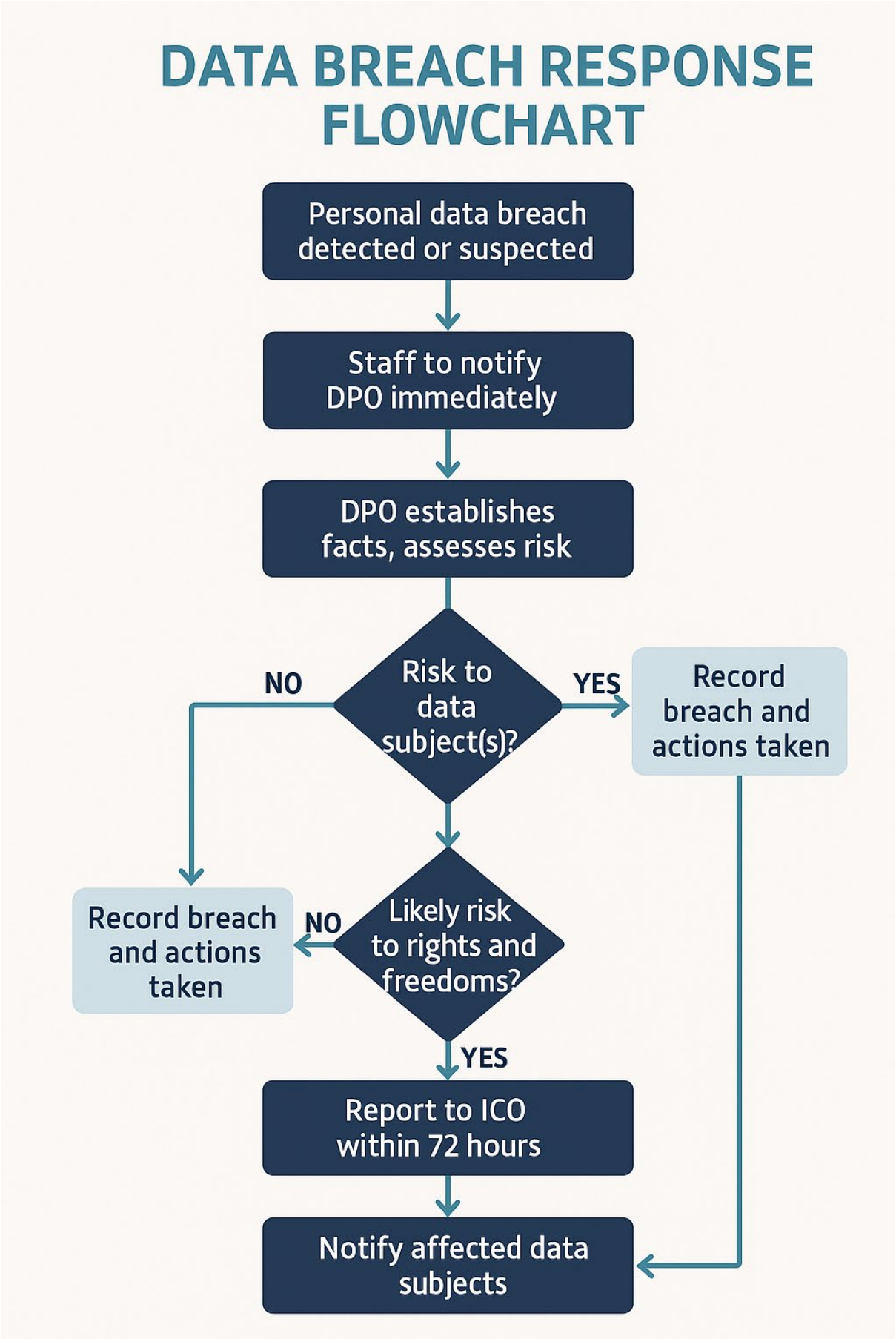
- Local authorities and partner agencies (e.g. health, social services)
- Educational settings, statutory bodies, or auditors
- Emergency services (when in the vital interests of a child)

Trauma-Informed Emphasis:

We recognise the heightened impact data misuse can have on children or staff who have experienced trauma:

- We treat information shared in confidence with respect, clarity, and secure handling.
- Data relating to identity, history of adversity, or therapy is processed with extra discretion.
- Data collection is done transparently, with explanation of how interventions or disclosures will be used and protected.

DATA BREACH RESPONSE FLOWCHART



1 Mandatory Induction Training (All New Staff)

- Introduction to GDPR and Data Protection Act 2018
- Updated UK Data Protection Regulations (including Children's Data & Online Safety Act 2023)
- AS2Educate's Data Protection Policy and Privacy Notices
- Recognising Special Category Data and Safeguarding Responsibilities
- Trauma-Informed Principles: Safety, Trustworthiness, Choice, Collaboration, Empowerment
- Handling Sensitive Information with Care and Empathy

2 Annual Refresher Training

- Key updates in legislation and AS2Educate procedures
- Data breach response protocol (linked to flowchart)
- Case studies on real-life data handling scenarios
- Trauma-informed responses when engaging with children, young people, and families
- Confidentiality vs. safeguarding: understanding when information must be shared lawfully

3 Specialist Training for Data Users and Leadership

- Role of the Data Protection Officer (DPO) and escalation process
- Data Protection Impact Assessments (DPIAs)
- Secure data storage and sharing protocols (including cloud-based solutions and encrypted communications)
- Supporting traumatised children and families when collecting or requesting personal information
- Information governance and accountability under Article 30 GDPR

4 Competency Checks & Record Keeping

- Staff knowledge checks and scenario-based quizzes

- Regular monitoring of adherence to policy
- Training logs maintained for audit and compliance purposes

5 Supportive Culture

- Ongoing supervision and guidance for staff managing sensitive data
- Open communication channels for raising concerns about data handling
- Embedding trauma-informed practice across all interactions with young people and families