

Attend Data Breach Policy

1. Purpose

This policy sets out the process for identifying, reporting, managing, and mitigating personal data breaches in accordance with UK GDPR and the Data Protection Act 2018.

2. Definition of a Data Breach

A personal data breach is defined as:

“A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.”

This includes breaches relating to confidentiality, integrity, or availability of data.

3. Scope

This policy applies to:

- All employees, contractors, and authorised users
- All systems and services operated by Attend
- All personal data processed on behalf of customers (schools)

4. Types of Data Breach

Examples include:

- Unauthorised access to systems or data
- Sending personal data to incorrect recipients
- Loss or theft of devices containing personal data
- System compromise (e.g. hacking, malware)
- Service outages affecting data availability

5. Responsibilities

- **All staff** must immediately report suspected breaches
- **Management** is responsible for assessing and responding
- **Data Protection Lead** (or equivalent) oversees compliance and notification

6. Breach Reporting Procedure

- **Step 1 – Identification**
 - Any suspected or actual breach must be reported immediately to:
 - internal management or designated contact
 - **Step 2 – Containment**
 - Immediate action should be taken to:
 - limit further data exposure
 - secure systems
 - prevent escalation
 - **Step 3 – Assessment**
 - The breach will be assessed to determine:
 - type and volume of data involved
 - sensitivity of data
 - number of individuals affected
 - potential risk to individuals

Attend Data Breach Policy

- **Step 4 – Notification**
 - **To the Customer (Controller)**
 - Schools will be notified **without undue delay**
 - **To the ICO**
 - If required, notification will be made within **72 hours** of awareness
 - **To Data Subjects**
 - Individuals will be informed (with cooperation of the Controller) where there is a **high risk to their rights and freedom**

7. Documentation

All breaches (including near misses) will be recorded, including:

- nature of the breach
- actions taken
- decisions regarding notification
- outcomes and lessons learned

8. Mitigation and Prevention

Following a breach, Attend will:

- implement corrective actions
- review policies and controls
- provide staff training where necessary

9. Security Measures

Attend maintains appropriate technical and organisational measures, including:


- access controls and authentication
- encryption where appropriate
- monitoring and logging
- secure hosting infrastructure

10. Review

This policy will be reviewed:

- annually
- or following any significant incident

Approved by A Cree, Director of Attend (trading as School Synergy limited).

Signature: 

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	A Cree	31/03/2026