



ASPIRE

CREATING INCLUSIVE EDUCATION

Data Protection Policy

Data Protection Policy

Aspire Behaviour Management (Aspire) is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, and parents.

1. Introduction

- a. Aspire needs to hold certain information about our employees, pupils, and other users to allow us, for example, to monitor performance, achievement, and health and safety.
- b. To comply with the law, information must be collected and used fairly, stored safely, and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles set out in the UK GDPR.
- c. In summary, these principles state that personal data shall:
 - i. Be obtained and processed fairly and lawfully.
 - ii. Be obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose.
 - iii. Be adequate, relevant, and not excessive.
 - iv. Be accurate and kept up to date.
 - v. Not be kept for longer than necessary.
 - vi. Be processed in accordance with the data subject's rights.
 - vii. Be kept secure against unauthorised access, loss, or destruction.
- d. All staff who handle personal data must follow these principles. This policy is not a contract of employment, but adherence is a condition of employment and breaches may lead to disciplinary action.

2. The Data Controller and Designated Data Controllers

- a. Aspire Behaviour Management is the Data Controller. The Directors are ultimately responsible for implementation.
- b. The Designated Data Controller is Michael Wood.
- c. Any concerns regarding data processing should be raised with the Managing Director in the first instance.

3. Responsibilities of Staff

All staff must:

- i. Ensure personal information they provide is accurate and up to date.
- ii. Notify Aspire of any changes (e.g. address or contact details).
- iii. Handle data in line with this policy.

4. Data Security

Staff are responsible for ensuring that personal data:

- i. Is securely stored (e.g. locked cabinet, encrypted storage).
- ii. Is not shared orally, in writing, or electronically with unauthorised parties.

Unlawful disclosure is a disciplinary offence and may constitute gross misconduct.

5. Rights to Access Information

Staff, parents, and data subjects have the right to:

- i. Know what information Aspire holds about them.
- ii. Request access to their data.
- iii. Request updates or corrections.
- iv. Understand Aspire's compliance with data protection law.

Requests for access should be made in writing to the Managing Director. Aspire may verify identity and reserves the right to charge a fee. Information will be provided within 30 days.

6. Retention of Data

Aspire retains certain personal data after employment or enrolment ends, primarily for legal, reference, or safeguarding purposes. Retention periods vary by data type.

7. Monitoring and Evaluation

This policy is reviewed annually or sooner if required. Any amendments will be reflected in the next version.

8. Last Review

This notice was last reviewed in July 2025 and will be reviewed annually or when significant changes occur.