



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 which are set out in 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 shall not be processed in any manner incompatible with that purpose.
 - iii. Be adequate, relevant and not excessive for that purpose.
 - iv. Be accurate and kept up to date.
 - v. Not be kept for longer than is necessary for that purpose.
 - vi. Be processed in accordance with the data subject's rights.
 - vii. Be kept safe from unauthorised access, accidental loss or destruction.
- d. All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, Aspire has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by Aspire from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2. The Data Controller and the Designated Data Controllers

- a. Aspire Behaviour Management, as a body, is the Data Controller under GDPR, and the Directors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.
- b. Aspire Behaviour Management has identified its Designated Data Controller as Michael Wood.



c. Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Principal, in the first instance.

3. Responsibilities of Staff

a. All staff are responsible for:

i. Checking that any information that they provide to the Aspire in connection with their employment is accurate and up to date.

ii. Informing Aspire of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. Aspire cannot be held responsible for any errors unless the staff member has informed Aspire of such changes.

iii. Handling all personal data (eg – pupil attainment data) with reference to this policy.

4. Data Security

a. All staff are responsible for ensuring that:

i. Any personal data that they hold or are given access to, is kept securely.

ii. Personal information, whether gathered by Aspire Behaviour Management or any other party, is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

b. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

c. Personal information should:

i. Be kept in a filing cabinet, drawer, or safe in a secure office, or;

ii. If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and

iii. If a copy is kept on a USB memory key or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

5. Rights to Access Information

a. All staff, parents and other users are entitled to:

i. Know what information Aspire holds and processes about them or their child and why.

ii. Know how to gain access to it.



iii. Know how to keep it up to date.

iv. Know what Aspire is doing to comply with its obligations under GDPR.

b. Aspire will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the Aspire holds and processes about them, and the reasons for which they are processed.

c. All staff, parents and other users have a right under GDPR to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. Aspire will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

d. Aspire may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

e. Aspire aims to comply with requests for access to personal information, as quickly as possible, but will ensure that it is provided within 30 days, as required by GDPR.

6. Retention of Data

a. Aspire has a duty to retain some staff and pupil personal data for a period of time following their departure from Aspire, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

7. Monitoring and Evaluation

This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review.

Date	Ratification	Reviewed by
February 2017	This policy was ratified by the board of Directors	Directors
August 2017	Updated	Lauren Bullock
April 2018	Updated – In line with GDPR	Michael Wood
April 2019	Reviewed – no changes	LB
December 20	Reviewed – no changes	LE