



Swallow Grange Alternative Provision

Data Protection (UK GDPR) Policy

Policy Owner: Head of Provision

Approved By: Footsteps to Futures Education Ltd

Date Approved: June 2026

Review Frequency: Annually

Next Review: June 2027

1. Statement of Purpose

Swallow Grange Alternative Provision is committed to protecting the privacy, confidentiality and security of all personal information entrusted to us.

As a specialist provision supporting children aged 4–11 with Special Educational Needs and Disabilities (SEND) and Social, Emotional and Mental Health (SEMH) needs, we recognise that we process significant amounts of sensitive personal information and have a responsibility to manage that information lawfully, fairly and securely.

This policy explains how Swallow Grange meets its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation.

2. Legal Framework

This policy has been developed with reference to:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Keeping Children Safe in Education (KCSIE)
- Education Act 2002
- Equality Act 2010
- ICO Guidance for Education Providers

3. Scope

This policy applies to:

- Pupils
- Parents and carers
- Employees
- Volunteers
- Governors
- Contractors
- Visitors
- Third-party processors

It covers all personal information processed in paper, electronic, photographic, audio or verbal formats.

4. Data Protection Principles

Swallow Grange will ensure personal information is:

- Processed lawfully, fairly and transparently.
- Collected for specified, legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date.
- Retained only for as long as necessary.

- Processed securely.
- Managed in a way that demonstrates accountability.

5. Roles and Responsibilities

Proprietor

The Proprietor Body has overall responsibility for ensuring compliance with data protection legislation.

Head of Provision

The Head of Provision will:

- oversee implementation of this policy;
- ensure staff receive appropriate training;
- monitor compliance;
- report significant breaches.

Data Protection Officer (DPO)

The Data Protection Officer will:

- advise the provision on GDPR compliance;
- monitor data protection arrangements;
- support Subject Access Requests;
- advise on Data Protection Impact Assessments;
- liaise with the Information Commissioner's Office (ICO).

All Staff

Every member of staff is responsible for:

- protecting confidential information;
- following school procedures;
- reporting data breaches immediately;
- completing mandatory training.

6. Personal Data We Process

Swallow Grange processes information relating to:

Pupils

Including:

- personal details;
- attendance;
- assessment information;
- EHCPs;
- safeguarding records;
- SEND records;
- behaviour records;
- medical information;
- photographs (where appropriate).

Parents and Carers

Including:

- contact details;
- emergency contacts;
- communication records;
- financial information where applicable.

Staff

Including:

- employment records;
- payroll;
- DBS information;
- qualifications;
- appraisal records;
- sickness records;
- pension information.

7. Lawful Bases for Processing

We process personal information under one or more of the following lawful bases:

- Public Task
- Legal Obligation
- Contract
- Vital Interests
- Legitimate Interests
- Consent (where required)

Special Category Data will only be processed where an additional lawful condition under Article 9 UK GDPR applies.

8. How We Collect Information

Information may be collected through:

- admissions documentation;
- employment processes;
- Local Authority referrals;
- previous educational settings;
- healthcare professionals;
- commissioning schools;
- day-to-day educational activities;
- safeguarding referrals;
- CCTV systems where installed.

9. How We Use Personal Data

Personal information is used to:

- educate and support pupils;
- safeguard children;
- meet statutory duties;
- monitor attendance and progress;
- provide SEND provision;
- communicate with parents;
- manage employment;

- administer payroll;
- ensure health and safety;
- manage finances;
- comply with inspection requirements.

10. Information Sharing

Personal information may be shared where lawful and necessary with:

- Local Authorities
- Department for Education
- NHS services
- CAMHS
- Social Care
- Educational Psychologists
- Speech and Language Therapists
- Ofsted
- Commissioning Schools
- Police
- Emergency Services
- Legal advisers
- Approved software providers

Information will only be shared where there is a lawful basis and only the minimum necessary information will be disclosed.

11. Information Security

Swallow Grange operates robust security measures including:

- password-protected systems;
- secure cloud-based platforms;
- encrypted devices where appropriate;
- locked filing cabinets;
- restricted staff access;
- visitor controls;
- secure disposal of confidential waste;
- regular backups;
- cyber security protection.

We currently use secure education systems including **CPOMS** for safeguarding records and **Bromcom** for management information.

12. CCTV

Where CCTV is installed it will be operated in accordance with the school's CCTV Policy.

Images will only be viewed by authorised personnel and retained for an appropriate period.

13. Data Retention

Information will only be retained for as long as necessary.

Retention periods are determined by:

- statutory requirements;
- ICO guidance;
- Department for Education guidance;
- operational need.

Records will be securely destroyed when no longer required.

14. Individual Rights

Individuals have the right to:

- be informed;
- access their information;
- request correction of inaccurate information;
- request erasure where appropriate;
- restrict processing;
- object to processing;
- request data portability where applicable;
- challenge automated decision making.

Requests will normally be responded to within one calendar month.

15. Subject Access Requests

Requests should be submitted to the Data Protection Officer.

Identity may be verified before information is released.

The school will respond within the statutory timescales unless an exemption applies.

16. Data Breaches

Any suspected data breach must be reported immediately to the Head of Provision or Data Protection Officer.

Where necessary the school will:

- investigate immediately;
- assess risk;
- notify the ICO within 72 hours where required;
- inform affected individuals where appropriate;
- implement measures to prevent recurrence.

17. Staff Training

All staff receive mandatory training covering:

- GDPR principles;
- confidentiality;
- cyber security;
- password management;
- recognising data breaches;
- information sharing;
- safeguarding confidentiality.

Refresher training is completed regularly.

18. Privacy Notices

Privacy Notices are provided to:

- parents;
- pupils where appropriate;
- staff;
- volunteers.

These explain:

- what information is collected;
- why it is collected;
- how it is used;
- who it is shared with;
- how long it is retained;
- individual rights.

19. Complaints

Anyone concerned about the handling of personal information should contact the Data Protection Officer in the first instance.

If they remain dissatisfied they may complain to the:

Information Commissioner's Office (ICO)

Website: www.ico.org.uk

Telephone: **0303 123 1113**

20. Monitoring and Review

This policy will be reviewed:

- annually;
- following changes in legislation;
- following ICO guidance;
- following any significant data breach.

Compliance will be monitored through:

- internal audits;
- staff training records;
- breach monitoring;
- governor oversight where appropriate.

21. Linked Policies

This policy should be read alongside:

- Privacy Notices
- Data Retention Schedule
- Freedom of Information Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Acceptable Use Policy
- Staff Code of Conduct
- CCTV Policy
- Records Management Policy

Approval

Approved by: Jayne Chudley

Position: Managing Director

Date: June 2026

Review Date: June 2027