Data Protection Policy

Policy Statement

Pavilion Pre-School (Aigburth) CIO is committed to protecting the privacy and personal data of all children, parents, staff, volunteers, and other stakeholders. This policy sets out how we collect, use, store, and protect personal data in compliance with UK data protection law, including the UK GDPR and the Privacy and Electronic Communications Regulations (PECR), incorporating the 2025 updates.

Scope

This policy applies to all personal data processed by Pavilion, whether in paper or electronic format, including:

- Children and parents/guardians
- Staff, volunteers, and contractors
- Suppliers and service providers

Key Principles

Pavilion will ensure that all personal data is:

1. Processed lawfully, fairly, and transparently.
2. Collected for specified, explicit, and legitimate purposes.
3. Adequate, relevant, and limited to what is necessary.
4. Accurate and kept up to date.
5. Kept only as long as necessary.
6. Processed securely, protecting against unauthorized access, loss, or destruction.

Data Protection Policy

Legal Basis for Processing

We process personal data on the following lawful bases:

1. Consent: Where individuals have given clear consent. This includes opt-in for marketing communications.

2. Contractual necessity: To provide childcare services or employment.

3. Legal obligation: To comply with statutory requirements.

4. Legitimate interests: Where necessary for operational purposes, such as maintaining a safe environment, recording attendance, or fundraising. Pavilion has documented our legitimate interest assessments to ensure balance with individual rights.

5. Soft opt-in (2025 update): For parents or staff with whom we have an existing relationship, we may send marketing or fundraising communications without explicit opt-in, provided the opportunity to opt out is clearly offered and the communications relate to similar services or activities.

Automated Decision Making

Pavilion does not use automated decision-making to make decisions with legal or significant effects on individuals.

Where automated decision-making is used (e.g., simple administrative workflows), it is limited to operational purposes and does not produce adverse effects on individuals.

Data Protection Policy

Data Minimisation and Retention

- Children's records, including developmental reports, are retained until the child leaves Pavilion plus 6 years.
- Staff records are retained for the duration of employment plus 6 years.
- Other personal data is retained only for as long as necessary for operational or legal reasons.
- All retention periods are reviewed annually.

Rights of Individuals

Parents, staff, and other stakeholders have the right to:

- Access their personal data
- Correct inaccuracies
- Object to processing on grounds of legitimate interests
- Request deletion of data where lawful
- Withdraw consent at any time
- Complain about the Pavilion's handling of personal data

Requests should be made to the Pavilion's Data Protection Officer (DPO).

Data Protection Policy

Complaints Process (2025 update)

Any individual may lodge a complaint regarding Pavilion's data processing. Pavilion Pre School (Aigburth) CIO will:

1. Acknowledge complaints within 30 calendar days.
2. Investigate complaints without undue delay.
3. Keep the complainant informed of progress
4. Provide an outcome without undue delay.
5. Inform individuals that they have the right to complain directly to the Information Commissioner's Office (ICO).

Electronic Communications and PECR Compliance

- All electronic marketing and fundraising communications comply with PECR.
- Soft opt-in communications are permitted where appropriate.
- Individuals can unsubscribe from electronic communications at any time.
- Higher fines under PECR (2025) for breaches are acknowledged, and compliance is a priority.

Data Security

Pavilion implements appropriate technical and organisational measures to protect personal data, including:

- Secure storage of paper records
- Password-protected electronic systems
- Restricted access based on role
- Regular staff training on data protection

Data Protection Policy

Data Sharing

Personal data will not be shared with third parties except:

- Where required by law or regulatory bodies
- With explicit consent
- For legitimate operational purposes (e.g., emergency services, safeguarding authorities)

All third-party contracts include data protection clauses.

Roles and Responsibilities

- Data Protection Officer (DPO): Oversees compliance and acts as point of contact.
- All staff: Must follow this policy and report breaches immediately.
- Management: Ensure regular training and monitoring.

This policy was adopted in October 2025 and will be reviewed annually or as required.
Last update: 08.07.26

Signed by Chair of Trustees:

Signed by Operations Manager: