Pace Data Protection Policy

Reviewed: July 2026
Next Review Date: September 2027
Reviewer: Director of Clinical Services
Approved: Chief Executive

Version	1.1	July 2026	SAR – Stop the clock Legal Framework section addition Version Control added Add in Data (Use and Access) Act 2025 (DUAA) amendments and references Updated contact number

Legal Frameworks

- UK GDPR
- Data Protection Act 2018
- DUAA 2025
- PECR
- Education legislation
- Safeguarding legislation
- Clinical governance standards
- Employment legislation
- Charity and fundraising requirements

Roles and Responsibilities

Board of Trustees

Overall oversight of data protection compliance and information governance.

Chief Executive / Data Protection Lead

Day-to-day responsibility for data protection compliance.

Policy development and review.

Training, advice and guidance.

Management of breaches, complaints and subject rights requests.

Managers

Monitoring compliance within their service areas.

Providing feedback and support to staff.

Escalating risks, incidents and concerns.

Staff and Volunteers

Compliance with data protection policies and procedures.

Protection of personal information.

Reporting breaches, incidents and concerns promptly.

Related Policies

Privacy Notices

Data Retention Policy

Complaints Policy

Overview

Pace takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. Pace is committed to a policy of protecting the rights and privacy of individuals in accordance with the Data Protection Act 2018 (the '2018 Act'), Data (Use and Access) Act 2025 and the UK General Data Protection Regulation ('UK GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

This policy applies to current and former employees, volunteers, pupils, parents, consultants, donors and any other individuals whose data we have collected. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. You should read this policy, where relevant, alongside your contract of employment or contract for services and any other notice we issue to you from time to time in relation to your data.

The organisation has a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The Charity its School, Therapy centre and subsequent departments have a duty to issue a Fair Processing Notice to all Stakeholders. This summarises the data which is held about individuals, why it is held and the other parties to whom it may be passed. The organisation has a data retention policy that details the location and retention period for all data held.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the 2018 Act and GDPR. It will apply to information regardless of how it is collected, used, recorded, stored, and destroyed and whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

Data Protection Principles

Personal data must be processed in accordance with six 'Data Protection Principles.' It must:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

We are accountable to these principles and must be able to show that we are compliant.

What is Personal data?

Personal information or data is defined as data that relates to a living individual who can be identified from that data or from that data and other information held by Pace. It includes any expression of opinion about the person and an indication of the intentions of us or others in respect of that person. It does not include anonymised data.

General Statement

Pace is committed to adhering fully to the data protection principles at all times. Therefore, Pace will:

- Inform individuals why the information is being collected when it is collected;
- Share information with others only when it is legally appropriate to do so;
- Inform individuals when their information is shared, and why and with whom it was shared via Privacy Notices
- Check the quality and the accuracy of the information it holds;
- Ensure that information is not retained for longer than is necessary;
- Ensure that when obsolete information is destroyed that it is done so fully, appropriately and securely;
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded;
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests (see Appendix 1);
- Ensure our staff are aware of and understand our policies and procedures in respect of data protection

Complaints

Data protection complaints will be handled in accordance with Pace's Data Protection Complaints Procedure.

Review

This policy will be reviewed annually, or sooner where legislative, regulatory or operational changes require.

The policy review will be undertaken by the Chief Executive, who is also the Data Protection Lead, or their nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact the Chief Executive/Data Protection Officer who will also act as the contact points for Subject Access Requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or by telephone on 0303 123 1113

Subject Access Request (SAR) Appendix

Overview

This policy outlines the procedures for handling Subject Access Requests (SARs) in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and the Data (Use and Access) Act 2025. It applies to all data subjects, including employees, donors, parents of children in therapy, and pupils.

Pace reserves the right to charge for or decline repeated, overlapping, excessive or manifestly unfounded requests.

Rights of Access to Information

Under the UK GDPR, any individual has the right to access personal data held about them. This includes employees, donors, parents, and pupils. Requests must be made in writing and addressed to the Data Protection Lead.

Actioning a Subject Access Request

1. Requests must be made in writing (including email) and addressed to the Data Protection Lead.
2. Identity verification is required. Acceptable forms include a passport, a driving license, a utility bill, etc.
3. Children aged 12 or older may be deemed competent to make their own request. Parental requests require consideration of the child's views.
4. No fee is charged unless the request is manifestly unfounded or excessive.
5. Where identity verification or clarification is reasonably required, the statutory timescale may be paused in accordance with applicable data protection legislation and will recommence once the required information has been received.
6. Some information may be exempt from disclosure.
7. Third-party data will not be disclosed without consent.
8. Information that may cause serious harm or relate to safeguarding or legal proceedings will not be disclosed.
9. Redacted copies will be retained for audit purposes.
10. Information must be clear and legible.
11. Delivery method will consider the applicant's preference. Secure methods will be used.

Data Subject-Specific Guidance

Employees

Employees may request access to personal data such as:

- Employment contracts
- Performance reviews
- Disciplinary records
- Emails or internal communications mentioning them

Confidential internal deliberations and third-party data may be redacted.

Donors

Donors may request access to:

- Contact details
- Donation history
- Communication preferences

Minimal redactions are expected unless third-party data is involved.

Parents of Children in Therapy

Parents may request access to their own data. Parents and or their legal representative may request the child's data. Examples include:

- Contact and consent forms
- Therapy session notes
- Communication records

Requests involving children's data require assessment of the child's capacity and may be restricted to protect the child's welfare or third-party confidentiality.

Complaints

Complaints should be directed to the Chair of Trustees. If unresolved, complaints may be escalated to the Information Commissioner's Office (ICO).

Contacts

For queries or concerns, contact the Chief Executive or Headteacher. Further advice is available from the ICO at www.ico.gov.uk or 0303 123 1113