

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') and the EU General Data Protection Regulation ('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.

Schools have 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. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents. This summarises the data which is held about pupils, why it is held and the other parties to whom it may be passed.

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 the way it is collected, used, recorded, stored and destroyed, and irrespective of 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 which relates to a living individual who can be identified from that data or from that data and other information that is 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;
- 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

Complaints will be dealt with in accordance with Pace's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Chief Executive, who is also the Data Protection Lead, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact Ian Sansbury (Chief Executive) or Claire Smart (Headteacher), 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 telephone 01625 5457453

Reviewed: September 2021
Next Review Date: September 2022
Owner: Chief Executive

Appendix 1

Pace Procedures for responding to subject access requests made under the 2018 Act and GDPR

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under 2018 Act and GDPR any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the 2018 Act and GDPR.

Actioning a subject access request

1. Data subjects can make a "subject access request" (SAR) to find out what information Pace hold about them. Requests for information must be made in writing (which includes email) and be addressed to the Data Protection Lead who will coordinate a response. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

5. The response time for subject access requests, once officially received, is one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months (**not working or school days but calendar days, irrespective of school holiday periods**). However, the one month will not commence until after clarification of information sought and proof of identity is obtained.

6. The 2018 Act and GDPR allows exemptions as to the provision of some information; **therefore, all information will be reviewed prior to disclosure.**

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the one-month statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at Pace with a member of staff on hand to help and explain matters if requested or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/ recorded mail must be used.

Complaints

Complaints about the above procedures should be made to the Chair of the Trustees who will decide whether it is appropriate for the complaint to be dealt with in accordance with Pace's complaint procedure.

Complaints which are not appropriate to be dealt with through Pace's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding these policies / procedures, then please contact the Chief Executive or Headteacher.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Covid-19 Policy Addendum

This notice describes how we may use pupils' personal information to protect them and others during the Covid-19 outbreak. It supplements our main Data Protection Policy, above.

If a pupil or parent has any concerns about our processing of personal data in relation to the COVID-19 pandemic, they should contact Ian Sansbury, our Chief Executive and GDPR Lead.

Safeguarding the health and safety of our pupils, members of staff and school community is of paramount importance.

During the COVID-19 pandemic we may process personal data in additional ways to ensure we are doing everything we can to protect everyone's health.

This may include:

- Asking whether pupils (or anyone in their households) are experiencing any COVID-19 symptoms.
- Collecting specific health data when someone tells us they are experiencing COVID-19 symptoms.
- Keeping a record of COVID-19 related health information.
- Analysing personal information already shared with us so we can ensure we are taking all possible measures to keep everyone safe.
- Sharing information with others; for example, with other members of a school 'bubble', Public Health, NHS Track and Trace system. When we process pupil personal information in this way, we will always abide by data protection law; namely, the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (UK DPA 2018).

Our processing will meet the principles laid down in the GDPR. This means that we will:

- Only collect and use the minimum amount of information that is necessary for the purpose of protecting the health and safety of pupils, and that of others.
- Make sure that any decisions we make about pupils based on this information are fair and don't discriminate against them.
- Only retain this information for as long as necessary. The retention period will be 12 months, but we will keep this under review.
- Ensure the security of pupils' personal information by adhering to the procedures laid down in our Data Protection Policy and IT/e-safety policies/user agreements.
- Share the minimum amount of personal information necessary for our purpose. We will do this verbally if appropriate, and will always seek not to share an individual's name unless it is absolutely necessary.

- Be open and transparent about our processing – through this addendum to our privacy notice and in any communications with pupils/parents.

Under the GDPR we must have a lawful basis to process personal data as described above. Our lawful basis is the one of 'public task', being processing that is necessary for our function as a school/ tasks in the public interest.

Due to its sensitivity, health information has extra protection under the GDPR and the UK Data Protection Act 2018 as special category data.

This means we have to identify an additional lawful condition for our processing: Our lawful condition is 'reasons of substantial public interest' under the GDPR and 'safeguarding of children and of individuals at risk' under Schedule 1, Part 2 of the UK DPA 2018.