



Partnership Achievement Community Excellence

---

## Data Protection Policy

---

Agreed by Directors:

---

Review Date: May 2019

---

# Contents

- What is the purpose of this policy? ..... 2
- Why do we collect and use data? ..... 3
- What data is covered by this policy? ..... 3
- What are the key principles and lawful reasons used to process data? ..... 3
- What personal data is collected? ..... 4
- What is meant by obtaining lawful consent? ..... 5
- Will personal data be shared? ..... 5
- How do we use photography and video? ..... 6
- Will personal data be published? ..... 6
- How long is personal data stored for? ..... 6
- Who is accountable for data protection? ..... 7
- How is personal data processed and protected? ..... 7
- What are your rights regarding your personal data? ..... 9
- What happens when there is a breach of your privacy? ..... 9
- How do you request access to view your personal data? ..... 9
- How do you raise a concern about the way we process personal data? ..... 10
- When will this policy be updated? ..... 10

## **What is the purpose of this policy?**

Under data protection legislation, PACE Academy Trust is the data controller of the personal information we hold. The Trust designates the Executive Head Teacher as its representative regarding the protection of data.

The postal address of the Trust is: c/o Chipstead Valley Primary School, Chipstead Valley Road, Coulsdon, Surrey CR5 3BW. For queries, please contact the school office on 01737 553255 or by email to; [office@chipstead.croydon.sch.uk](mailto:office@chipstead.croydon.sch.uk)

The Trust is required to keep and process personal information about its pupils, families and staff in accordance with its legal obligations. This information will be processed in accordance with the EU General Data Protection Regulation 2018 (GDPR).

The Trust may, from time to time, be required to share personal information with other organisations, including the Local Authority (LA), Department for Education (DfE,) other schools, and relevant bodies who provide services to the school.

This policy will outline the legal framework, practices and processes used in the Trust with regards to the proper collection, processing and retention of personal data we hold.

A summary of this Data Protection Policy is provided in our Privacy Notices which can be downloaded from the Trust website; [www.paceacademytrust.com](http://www.paceacademytrust.com) or are available on request from the school offices.

This document is a working document and will be regularly updated, (at least once per year) to reflect changes in the working practices of the trust. Please ensure that you access the most recent version of this document either through the website or by contacting the school offices.

## Why do we collect and use data?

PACE Academy Trust is a publicly funded body responsible for providing state education of children. The Trust is required by law to comply with legislation including, but not limited to, the following:

- The Education (Pupil Information) (England) Regulations 2005 (amended 2016)
- The School Standards and Framework Act 1998
- The General Data Protection Regulation 2018 (GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy will underpin all data processing activities within the trust and makes reference to the following other trust policies:

- E-safety Policy
- Safeguarding Policy
- Document Retention Policy
- Whistleblowing Policy

The Trust uses the information it holds in order to:

- Support the teaching and learning of pupils and staff
- Monitor and report on progress and achievement
- Provide appropriate care and safeguarding for pupils and staff
- Assess the quality of our service
- Comply with our legal obligations

## What data is covered by this policy?

The Trust recognises the following categories of data which are collected and processed by the individual schools. This policy applies to both personal data held electronically and data stored in paper records in our filing systems. Personal data may be processed according to specific criteria, including chronologically ordered data and data which has been pseudonymised.

**Personal data** is information that relates to an identifiable, living individual, this can include information relating to online identity such as usernames or IP addresses.

**Sensitive personal data** is defined as a special category of personal data (refer to GDPR Article 9). This can include the processing of genetic data, biometric data and data concerning health matters. The Trust applies additional measures to protect and secure this type of data.

**Criminal convictions and offences** are another example of personal data, but which are not included under the category of sensitive personal data. The Trust applies additional safeguards to the processing of this data (refer to GDPR Article 10).

## What are the key principles and lawful reasons used to process data?

The Trust will ensure that all personal data is only ever collected, processed and stored according to the key principles identified in the GDPR to ensure that privacy and data security is embedded within the

culture of the organisation at all levels. The trust recognises that personal data may only be processed lawfully, the lawful reasons used by the trust are identified as follows:

- To allow the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller to carry out the duties of the trust
- To protect the vital interests, health or wellbeing of an individual
- To comply with legal obligations
- To deliver a contract, or to take steps required to enter in to a contract
- To undertake other legitimate interests pursued by the Data Controller or a third party
- With the consent of the person concerned, which has been legally obtained

### **What personal data is collected?**

The trust can collect and process the following personal data relating to pupils or their families:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth, religion, free school meal eligibility and photographs for identification
- Attendance information including absences and absence reasons
- Assessment information including National Curriculum assessment results and scores used to measure learning, development and progress
- Medical history and information relevant to health and wellbeing such as allergy information
- Information relating to identified Special Educational Need and Disability (SEND)
- Behavioural information including exclusions and incident reports
- Safeguarding information relating to protecting the safety or best interest of children including care and social services data, legal or judicial communications and information supplied by related agencies

The Trust can collect and process the following personal data relating to its employees and governors:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth and photographs for identification
- Attendance information including absences and absence reasons
- Employment and Contractual information such as qualifications, criminal records checks, references, employment history, trade union membership, religion and financial data such as bank details and tax information
- Medical history and information relevant to health and wellbeing such as disability or allergy information
- Performance Management information such as appraisals or disciplinary records

The Trust can collect and process the following personal data relating to contractors and visitors:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth and photographs for identification
- Employment and Contractual information such as qualifications, criminal records checks, references, employment history, trade union membership, religion and financial data such as bank details and tax information

## **What is meant by obtaining lawful consent?**

The schools within the trust may identify additional uses of your data, which may be of benefit to your child or the school community. Examples may include optional extra-curricular activities, fundraising or school promotional activities. We will always seek your consent before using your data for these reasons. If you give consent, you may change your mind at any time.

Individual schools will provide consent forms at admission, these can also be found on the school websites. An opt out form is available on school websites and in the school offices, forms should be returned to the school office.

## **Will personal data be shared?**

The Trust is legally obliged to share data about pupils and staff with the Department for Education (DfE). The DfE use this data for school funding and educational attainment policy and monitoring.

The DfE routinely request data throughout the year which include the School Census return and Early Years Census. To find out more about the pupil information we share with the DfE for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Some of this information is then stored on the National Pupil Database (NPD), which is permitted in law by the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD please go to: <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

The DfE may share information about pupils from the NDP with third parties who promote the education or wellbeing of children through research, providing information, advice or guidance.

To find out more about information about the DfE's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Individual schools and the Trust will also share personal data with approved third parties or contractors in order to deliver its aims.

The information shared may include sensitive personal information such as information about health, special educational needs, or disabilities. This information is used to provide the correct services to support children, families or employees and is only shared on a strictly need to know basis in full compliance with individual's rights.

The trust is required by law to check the identity and Criminal Record of all employees, governors and volunteers in order to safeguard children and staff.

The trust will conduct checks using the Disclosure and Barring Service (DBS). In order to carry out these checks, it is required for authorised persons to share sensitive personal data with the DBS.

Personal Data will be processed by the DBS and the results of this processing provided to the school. You may review the privacy notices provided by the DBS for further information on the gov.uk website. <https://www.gov.uk/government/organisations/disclosure-and-barring-service>

## **How do we use photography and video?**

The Trust recognises that the recording images of identifiable individuals is a form of processing personal information which must be carried out in line with data protection requirements.

The Trust makes use of CCTV systems in order to provide enhanced security of the premises and to better safeguard the interests of pupils and staff. In schools where CCTV is used the rules are followed;

- The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All CCTV footage will be kept for 30 days for security purposes; the Office Administrator and SBM/SBO are responsible for keeping the records secure and allowing access.

The school captures photographs of pupils, staff, contractors and visitors to our site for the purposes of identification and authorisation of access. These images may be further processed and linked to other information we hold such as emergency medical needs, or attendance records.

The schools within the trust may use photography and video images for other explicit purposes in order to deliver its aims. Full details of these purposes are outlined in our policy below.

- The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
- Precautions, as outlined in the Photography and Videos at School Policy, are taken when publishing photographs of pupils, in print, video or on the school website.
- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## **Will personal data be published?**

The Trust will not publish any personal data, including photos or images, in a public forum either online or in print without obtaining explicit consent in advance.

## **How long is personal data stored for?**

Personal data held by the Trust is stored and deleted according to our **Data Retention Policy**.

Personal data is not kept on a permanent basis and is only stored for as long as is necessary to fulfil its intended purpose. Personal data is deleted when it is no longer required. Some educational records relating to former pupils or employees of the trust may be kept for an extended period for legal reasons, but also for example to enable the provision of references.

Paper documents will be shredded or securely disposed of, and electronic data scrubbed clean or permanently erased once the data is no longer required.

Please review our Data Retention Policy for further details of specific data items and their retention schedules.

### **Who is accountable for data protection?**

Under data protection legislation, the trust is the Data Controller of the personal data we hold.

The GDPR requires that the Data Controller shall be responsible for, and able to demonstrate, compliance with the principles outlined above. The trust designates the Executive Head Teacher as its representative with regards to data protection.

As a publicly funded body the Data Controller is required to appoint a Data Protection Officer (DPO).

The trust has appointed OpenAIR Systems Limited as its DPO. The DPO can be contacted by email [dataprotection@openair.systems](mailto:dataprotection@openair.systems) or in writing to OpenAIR Systems, Unit 20 Capital Business Centre, 22 Carlton Road, Croydon CR2 0BS.

The DPO has a range of responsibilities which support the trust in meeting its obligations under GDPR. The DPO will act as a point of contact and adviser to the trust, its employees and clients.

### **How is personal data processed and protected?**

The trust ensures appropriate technical measures and processes are in place to protect data and privacy of individuals. The trust defines comprehensive, understandable and transparent policies which give due regard to the protection and security of data. Policies underpin the culture and behaviours adopted by the trust and outline our business processes and structure. All policies are reviewed on a regular basis to ensure they reflect the most up to date circumstances and any changes in working practice. When reviewed, all policies are checked alongside this data protection policy to ensure a comprehensive and integrated approach to privacy is delivered.

The trust maintains a Data Protection Audit as an internal record of all data processing activities carried out, and reviewed at least once per year to ensure the content is kept up to date. The audit includes full itemised details of each data processing activity, nature and categories of data, reasons for processing and the systems used to carry out the processing.

When introducing new systems or new ways of processing personal data, the trust and its schools will conduct a Data Protection Impact Assessment (DPIA) in order to ensure proper integration and compliance with the law and our policies. Any new systems implemented by the school will ensure data protection is implemented by design and privacy enabled by default.

In order to ensure that data is protected, the trust has identified the following measures which are implemented to minimise the risks involved in processing and storing information.

Staff and Governor responsibilities;

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access or on unattended desks, papers should be locked away at night.
- Filing cabinets and cupboards containing personal information will be kept locked when unattended.
- Computer screens should be locked (windows/L) when leaving the desk unattended and turned off at the end of the day and during holidays.



- Files of pupils leaving the school will be sent by recorded delivery or hand delivered and signed as received by the future school.
- Disposal of personal information following the retention period will be shredded or disposed of through a confidential waste contractor.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors will not use their personal laptops or computers to store or process any personal data or sensitive data.
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- When sending confidential information by email, staff will always check that the recipient is correct before sending and that no personal data or email addresses are within the body of the email.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. Paper based information should be kept confidential and secure when in transit and transported in a sealed file or envelope. The person taking the information from the school premises accepts full responsibility for the security of the data and will report any loss to the Head Teacher/Head of School immediately.
- Before sharing data, all staff members will ensure:
  - They are allowed to share it.
  - That adequate security is in place to protect it.
  - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- PACE Academy Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Executive Head Teacher is responsible for continuity and recovery measures are in place to ensure the security of protected data.

All third parties working at the school must

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the trust, are aware of this policy and are fully trained in and are aware of their duties under GDPR. Any breach of any provision of GDPR will be deemed as being a breach of any contract between the trust and the individual, company, partner or firm.
- Co-operate with data protection procedures and audits undertaken by the trust or its schools.

## **What are your rights regarding your personal data?**

The trust recognises the rights of individuals with regards to our use of their personal data, a list of your rights are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

The trust will ensure that these rights are respected by ensuring that all our policies and processes regarding data processing and data storage are compatible with these rights.

In addition to the rights detailed above, individuals have further rights relating to the automated processing of their personal data.

The trust does not make use of any automated decision making in the processing of data, neither does it undertake automated profiling of individuals.

## **What happens when there is a breach of your privacy?**

The Trust will use practical and technical measures to protect personal data from loss or any other unauthorised alteration, disclosure, or access.

In the event of a breach of privacy as described above, the Head Teacher in consultation with the DPO, will take the following action:

- Assess the nature of the personal data breach, including the categories of data concerned and approximate number of individuals and records affected
- Identify if the breach is likely to result in any risk to the rights and freedoms of individuals. Risk of the breach having a detrimental effect on individuals, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis
- Report all notifiable breaches to the Information Commissioners Office within 72 hours of the trust becoming aware of it
- If a breach is likely to result in a high risk to the rights and freedoms of an individual, the trust will notify those individuals concerned directly and without undue delay

## **How do you request access to view your personal data?**

Under data protection legislation, any individual about whom the trust processes personal data (the Data Subject) has the right to request access to view the information that we hold about them.

Requests for access to your personal information must be recorded in writing, this is known as a Subject Access Request (SAR).

You may make a request verbally by speaking to a member of staff who will record your request.

Alternatively, you may use our Subject Access Request Form or write your own letter addressed to the Head Teacher sent care of our nominated DPO; OpenAIR Systems, Unit 20 Capital Business Centre, 22 Carlton Road, Croydon, CR2 0BS, or submit an emailed a request to the relevant school;

Chipstead Valley Primary	<a href="mailto:chipstead.sars@openair.systems">chipstead.sars@openair.systems</a>
New Valley Primary	<a href="mailto:newvalley.sars@openair.systems">newvalley.sars@openair.systems</a>
Beecholme Primary	<a href="mailto:beecholme.sars@openair.systems">beecholme.sars@openair.systems</a>
PACE academy	<a href="mailto:paceacademy.sars@openair.systems">paceacademy.sars@openair.systems</a>

You will receive an automated acknowledgement of the receipt of your request when sent via email. All SAR requests will be processed in accordance with GDPR requirements.

### **How do you raise a concern about the way we process personal data?**

If you have a concern about the way we collect or use your personal data, we invite you to raise the matter with us in the first instance, either by contacting the trust, school, or via our DPO.

Alternatively, you can contact the Information Commissioner's Office:

By post to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

By telephone: 0303 123 113 or 01625 545 745, or online at <https://ico.org.uk/concerns>

### **When will this policy be updated?**

This policy will be reviewed at least once per year by the Trust.

This policy is a working document and can be updated to reflect changes in the working practices of the Trust at any time. Please ensure that you access the most recent version of this document either by downloading the current version the website or by contacting the school office.

The next scheduled review date for this policy is May 2019