Privacy Notice for Parents/Carers – use of your child’s personal data

This Privacy notice is to help parents understand how and why Penwortham Primary collects your child’s personal information and what we do with that information. Under the new the General Data Protection Regulations (GDPR) coming into effect on 25th May 2018, individuals have a right to be informed about how the school uses any personal data that we hold about them.

This privacy notice explains how we collect, store and use personal data about pupils.

Our data protection officer is **Gary Hipple, Head of schools IT in Wandsworth**.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion and behaviour information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs and videos
- CCTV images captured in school
- Sporting fixtures and other news on the website
- Trips and transport
- School transfer forms
- Paper records and virtual learning environments

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
Our legal basis for using this data

We only collect and use pupils’ personal data when the law allows us to. Most commonly, we process it where:
- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils’ personal data in situations where:
- We have obtained consent to use it in a certain way
- We need to protect the individual’s vital interests (or someone else’s interests)

Where we have obtained consent to use pupils’ personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils’ personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. The Information and Records Management Society’s toolkit for schools sets out how long we keep information about pupils.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil’s family and representatives
- Educators and examining bodies
- Our regulator e.g. Ofsted.
- Suppliers and service providers – to enable them to provide the service we have contracted them for. This includes organisations such as Place2Be, Target Tracker, Tapestry, Wandsworth Music Service, CPOMs, School Cloud, SIMs and Penwortham Out of School Care
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
Professional advisers and consultants
Charities and voluntary organisations
Police forces, courts, tribunals
Professional bodies

National Pupil Database
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally
Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data
Individuals have a right to make a 'subject access request'- subject access is to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child’s data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you or your child, we will:
- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Present the information

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances. Parents/carers also have a legal right to access to their child's educational record.

If you would like to make a request please contact our data protection officer, Gary Hipple.
ghipple@wandsworth.gov.uk

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:
- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
• In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
To exercise any of these rights, please contact our data protection officer.

Complaints and contact
We take any complaints about our collection and use of personal information very seriously.
If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.
To make a complaint or if you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

• Gary Hipple

This notice is based on the Department for Education’s model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.
Appendix 1

School Data Breach Procedure

Data Protection - Data Breach Procedure for Penwortham Primary School

Policy Statement
Penwortham holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Penwortham and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by all staff at Penwortham if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

**Types of Breach**

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

**Managing a Data Breach**

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher or the School’s Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School’s legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

   a. Attempting to recover lost equipment.
b. The use of back-ups to restore lost/damaged/stolen data.

c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation
In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner’s Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification
Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

Review and Evaluation
Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next
available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School’s Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School’s Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.
Subject Access Request Procedure for Schools

Scope
All personal data processed by Penwortham Primary School or on behalf of Penwortham Primary School is within the scope of this procedure.

Data subjects are entitled to obtain:
- Confirmation as to whether Penwortham Primary School is processing any personal data about that individual;
- Access to their personal data;
- Any related information;

Procedure
Subject Access Requests (SARs) for information must be made in writing and sent to Mrs Andrews, Headteacher. The school will provide a template for the request (appendix 3).

If an individual is unable to provide a request in writing and justifiable assistance is required, it must be provided and the request can be made on behalf of the individual.

Penwortham Primary School does not need to respond to a request made orally but, depending on the circumstances, it might be reasonable to do so (as long as the school is satisfied about the person’s identity). It is good practice at least to explain to the individual how to make a valid request, rather than ignoring them.

If a request does not mention the Data Protection Legislation specifically or even say that it is a subject access request, it is nevertheless valid and should be treated as such if it is clear that the individual is asking for their own or child’s personal data.

Requesters do not have to tell Penwortham their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.

A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So it is important to ensure you recognise a subject access request (SAR) and forward it to the named person in school who will liaise with the school Data Protection Officer.

Any school employee who receives a request for a subject access request (SAR) must forward it immediately to Mrs Andrews, Headteacher, no matter what form it is received in.

Mrs Andrews will log and acknowledge the request.

The data subject will provide the school with evidence of their identity and the signature on the identity must be cross-checked.

List of acceptable identity includes:
- Passport
- Driving licence
- Birth certificate
- Utility bill (from last 3 months)
- Current vehicle registration document
- Bank statement (from last 3 months)
- Rent book (from last 3 months)
- Council tax

The data subject may specify to Penwortham Primary School a specific set of data held by Penwortham on their subject access request (SAR). The data subject can request all data held on them.

Mrs Andrews will update the log and record the date that the identification checks were conducted and the specification of the data sought.

Diane Watkins, SBM and Emma Berner, Computing Lead will work with the school Data Protection Officer to provide the requested information to the data subject within one month from this recorded date.
Under the GDPR Article 12 (3), the month deadline may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Mrs Andrews shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Example of reason for the delay:
- Volume of information is over 1,000 pages
- Open complex cases
- Three or more third parties are included

Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Once received, the subject access request (SAR) is immediately forwarded to Mrs Andrews, who will ensure that the requested data is collected within the specified time frame.

Collection entails:
- Collecting the data specified by the data subject,
- Request Penwortham to search and retrieve information from all relevant databases and all relevant filing systems (manual files) in the school, including all back up and archived files (computerised or manual) and all email folders and archives.

The Data Protection Officer will maintain a record of requests for data and of its receipt, including dates and copies of correspondences.

All documents should be reviewed that have been provided, to identify whether any third parties are present in it, and either remove the identifying third party information from the documentation or obtain written consent from the third party for their identity to be revealed.

The DPA currently sets out a number of exemptions which allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed.

Current exemptions which are relevant include:
- Confidential references – schools do not have to provide subject access to references they have confidentially given in relation to an employee’s employment;
- Management information – personal data which relates to management forecasting or planning is exempt from subject access (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation);
- Legal advice and proceedings – schools do not have to disclose data which is covered by legal professional privilege;
- Settlement negotiations – the subject is not entitled to personal data which consists of a record of the employers intentions in respect of settlement discussions that have taken place or are in the process of taking place with that individual.

In the event that a data subject requests details of what personal data is being processed then they should be provided with the following information:

- Purpose of the processing
- Categories of personal data
- Recipient(s) of the information, including recipients in third countries or international organisations
- How long the personal data will be stored
- The data subject’s right to request rectification or erasure, restriction or objection, relative to their personal data being processed.
- Penwortham takes appropriate measures to act without undue delay in the event that the data subject has: withdrawn consent (objects to the processing of their personal data in whole or part; no longer under legal obligation and/or has been unlawfully processed.
Inform the data subject of their right to lodge a complaint with the ICO and a method to do so.

Inform the data subject of any automated decision-making.

If and where personal data has been transferred and information on any safeguards in place.

Penwortham does not charge a fee for Subject Access Requests (SARs).

**Complaints against Subject Access Requests (SARs)**

Individuals that wish to make a complaint about the handling of their Subject Access Request (SAR) can raise a concern with the Data Protection Officer. They also have a right to raise their concern with the Information Commissioner’s Office. Any Subject Access Request (SAR) concern received by a school employee must be forwarded to the Data Protection Officer immediately.
Re: subject access request

Dear Penwortham Primary School,

Please provide me with the information about me that I am entitled to under the Data Protection Act 2018 and General Data Protection Regulation (GDPR). This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

<table>
<thead>
<tr>
<th>Name</th>
<th>Please select:</th>
<th>Other (please specify):</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Relationship with the school</th>
<th>Please select:</th>
<th>Pupil / parent / employee / governor / volunteer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correspondence address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Details of the information requested

*Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:*

- Your personnel file
- Your child’s medical records
- Your child’s behavior record, held by [insert class teacher]

*Emails between ‘A’ and ‘B’ between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within 1 month.

If you need any advice on dealing with this request, you can contact the Information Commissioner’s Office on 0303 123 1113 or at [www.ico.org.uk](http://www.ico.org.uk)

Yours sincerely,

Mrs Andrews

Headteacher