Withinfields Primary School

Data protection policy

1. Aims

Withinfields Primary School aims to ensure that all personal data collected about staff, pupils, parents, carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018)

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO)

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. The data controller

Withinfields Primary School processes personal data relating to parents, carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. Our ICO registration number is Z7085634

4. Roles and responsibilities

This policy applies to **all staff** employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1. Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

4.2. Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is The Valley Learning Partnership, contactable via the school office.

4.3. Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

4.4. All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

5. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles

6. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will meet one of the special category conditions for processing which are set out in the Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools

8. Sharing personal data

We will share personal data with statutory bodies, such as the Department for Education and Local Authority where we are required to do so. We will share personal data if;

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent if necessary
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement agencies where we are legally required to do so.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

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.

9. Individuals rights

9.1. Data protection rights of the individual

Individuals also have the right to:

- Access to their personal data and supplementary information
- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest

- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO via the school office. If staff receive such a request, they must immediately inform the DPO.

9.2. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO via the school office. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO via the school office.

9.3. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.4. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Protecting and Safeguarding children policy for more information on our use of photographs and videos.

13. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

15. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

During the first year of implementation this policy will be under review as guidance from the ICO and DfE is released. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

17. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Data retention schedule
- Acceptable use of ICT policy
- Protecting and Safeguarding Children policy

Appendix 1 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Appendix 2 – Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Head Teacher/Business Manager.
2. The staff member or data processor will be asked to complete the school's data breach form.
3. The Head Teacher/Business Manager will assess the nature of the breach and make an initial entry in the school's breach register.
4. The Head Teacher/Business Manager will inform the DPO of the potential breach
5. On receiving the breach report, the DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    a. Lost
    b. Stolen
    c. Destroyed
    d. Altered
    e. Disclosed or made available where it should not have been
    f. Made available to unauthorised people
6. The DPO will keep the headteacher informed throughout the process
7. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
8. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
9. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    a. Loss of control over their data
    b. Discrimination
    c. Identify theft or fraud
    d. Financial loss
    e. Unauthorised reversal of pseudonymisation (for example, key-coding)
    f. Damage to reputation
    g. Loss of confidentiality
    h. Any other significant economic or social disadvantage to the individual(s) concerned
    i. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the breach being reported.
10. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are recorded within the school breach register.
11. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    a. A description of the nature of the personal data breach including, where possible:
        i. The categories and approximate number of individuals concerned
        ii. The categories and approximate number of personal data records concerned
    b. The name and contact details of the DPO
    c. A description of the likely consequences of the personal data breach
    d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

12. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
13. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a. Facts and cause
    b. Effects
    c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
15. Depending on the severity of the breach, the DPO and headteacher will either discuss the outcome over the phone or meet to review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

Appendix 3 – Data Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the School Business Manager or Headteacher immediately. The breach will be recorded on the School's Breach Register and the DPO informed so that an investigation can be carried out		
	Report by:	
	Date	
1	Nature of breach e.g. theft/disclosed in error/technical problem	
2	Description of how breach occurred:	
3	When was the breach reported and how did you become aware?	
4	Full description of all personal data involved	
5	Number of individuals affected? Have all individuals affected been informed	
6	What immediate remedial action was taken:	
7	Has the data been retrieved or deleted? If yes – date and time:	
8	Any Procedure changes needed to reduce risks of future data loss	
9	Conclusion	

Appendix 4 – Subject Access Request Form

Personal information collected from you by this form, is required to enable your request to be appropriately processed, this personal information will only be used in connection with the processing of this Subject Access Request.

This form is only to be used when making an application for personal data held by Withinfields Primary School

Please note: Before logging your request, we will require proof of identity by production of a passport, photo-driving licence, or a utility bill in your name and current address. Please supply your proof of identity when making your application. A scanned or photocopied copy will be sufficient.

Name	
Address	
Previous Address: (If Applicable)	
Date of Birth:	
Contact Phone number:	
Email Address:	
Details of information requested:	

Parent applying on behalf of a child

If you are a parent applying for access on behalf of your child, please complete the following and tick the relevant box.

Please note that you must be able to establish that you are legally able to act on behalf of your child. This generally means that you must have parental responsibility for him or her. It should be noted that a parent can only be granted access to their child's records if this is considered to be in the child's interests.

Name of child	Date of Birth

I (Name of parent) ..... am making a request for access to records on behalf of the child named above and:

Tick as appropriate:

The child is incapable of understanding the request and I am making the request on his/her behalf ☐

The child has consented to my making this request on his/her behalf and this consent was freely given ☐

Childs signature (where consent is given)	Date

Applicants signature

I declare that the information given be me is, to the best of my knowledge correct and that I am entitled to apply for access to the information referred to above, under the terms of the Data Protection Act 1998.

Signature:	Date of Request:

Once Withinfields Primary School has received all the required information, your request should be completed within one month. In exceptional circumstances where it is not possible to comply within this period you will be informed of the delay and given a timescale for when your request is likely to be met.

Please return this form to:

Address of school

Please note:

- The school may contact you for further clarification regarding the information required.
- Once the information has been collated, you will be notified that your file is ready for collection or to be sent securely.

For schools use only

Form of ID Provided	Date Request Received
Date Request Acknowledged	Target Date for Completion of SAR