Annual Policy for Data Protection/GDPR and Privacy Notice

Dry Sandford Primary School

Leading Lifelong Learning; Creating Caring Communities

Aims: Dry Sandford Primary School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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

Data protection principles

The UK 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 including our privacy notice

Privacy Notice – Parents/Carers

The categories of parent/carer information that we process include:

Personal information (such as name, address, phone numbers and email address)
Characteristics (such as gender and first language)

Why we collect and use parent/carer information

We collect and use this information, for the following purposes:
To meet our statutory requirements
To help keep children safe whilst in our care
To aid communication between school and home.
The Lawful bases we rely on for processing pupil information are:

Under Article 6 (1) of the General Data Protection Regulation, “Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority invested in the controller”.
Special category data is processed under Article 9 (2) (b) of the General Data Protection Regulation: “Processing is necessary for the purposes of carryout the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law providing for the appropriate safeguards for the fundamental rights and the interests of the data subject”.

How we collect parent/carer information

Whilst the majority of pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the General Data Protection Legislation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store parent/carer data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please

Who we share parent/carer information with

We routinely share information with:

- Schools that your child attends after leaving us
- Our Local Authority
- Health Authority
- The Department for Education (DfE)
- Sims– the School’s management Information System)
- Microsoft 365 (email communication)

We also share limited information with the following organisations

- Eduspot, Class Dojo, MS Teams (our correspondence systems)
- Schools Money (our online payment system)

Why we regularly share pupil information

Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- 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 as 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 UK data protection law
- Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
- We will also share personal data with law enforcement and government bodies where we are legally required to do so.

- We may also share personal data with emergency services and local authorities to help them respond to an emergency that affects any of our pupils or staff.
- Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals Under data protection legislation, parents/carers have the right to request access to information about them that we hold about them.

This request is known as a Service Access Request.(SAR) To make such a request for this please contact The School Business Manager in writing.

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.

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 (or receipt of the additional information needed to confirm identity, where relevant)

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 may not disclose information for a variety of reasons, such as if it:

Might cause serious harm to the physical or mental health of the pupil or another individual

Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests

Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it

Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress

- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

Data security and storage of records

- We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
- In particular:
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT acceptable use policy on acceptable use.)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

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.

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 after becoming aware of it. 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

Training

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary. All staff and governors are provided with data protection training as part of their induction process.

Monitoring arrangements:

The Data Protection Officer DPO (Helen Lyons) is responsible for monitoring and reviewing this policy.
This policy will be reviewed annually and approved by the full governing board.

Links with other policies

This data protection policy is linked to our:

Freedom of information publication scheme
Safeguarding policy
If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/Contact
If you would like to discuss anything in this privacy notice, please contact The School Business Manager

Headteacher signed: KFriday Chair of Governors signed:

Reviewed: May 2024

Review date: annually May 2025