



Data Protection Policy

1. Aims

Findon Village Pre-School aims to ensure that all personal data collected about staff, children, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018).

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) on the GDPR and the ICO's code of practice for subject access requests. 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. Definitions

Term	Definition
Personal Data	<ul style="list-style-type: none"> • Any information relating to an identified, or identifiable, individual. <p>This may include the individual's:</p> <ul style="list-style-type: none"> • 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.
Term	Definition
Special categories of personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions

	<ul style="list-style-type: none"> • Religious or philosophical beliefs • Trade union membership • Genetics • Health – physical or mental • Sex life or sexual orientation
Term	Definition
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.
Term	Definition
Data subject	The identified or identifiable individual whose personal data is held or processed.
Term	Definition
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Term	Definition
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.
Term	Definition
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Findon Village Pre-school processes personal data relating to parents, children, staff, trustees, visitors and others, and therefore is a data controller. The Pre-School is registered as a data controller with the ICO and will renew this registration every 2 years or as otherwise legally required.

Registration number: ZA661991

5. Roles and responsibilities

This policy applies to all staff employed by our pre-school, and to external organisations or individuals working on our behalf.

5.1 Pre-School Trustees

The Pre-School trustee's overall responsibility for ensuring that our Pre-School complies with all relevant data protection obligations.

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

Our DPO is Andrew Stowell (Trustee) and is contactable via the main pre-school email: fvpreschool@gmail.com

5.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the Pre-School of any changes to their personal data, such as a change of address.

Staff must contact 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
- 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.

6. Data protection principles

The GDPR is based on data protection principles that our Pre-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 Pre-School aims to comply with these principles.

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 Pre-School can fulfil a contract with the individual, or the individual has asked the Pre-School to take specific steps before entering into a contract.
- The data needs to be processed so that the Pre-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 Pre-School 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 Pre-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 also meet one of the special category.

7.2 Limitation, minimisation and accuracy

The Pre-School 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.

8. Sharing personal data

The Pre-School will not normally share personal data with anyone else, but may do so 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 before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

When sharing data with suppliers or contractors, 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 and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud.

- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

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.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Pre-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 or email to the DPO. 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.

9.2 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, subject access requests from parents or carers of pupils at our Pre-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.

9.3 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 considers 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.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- 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.
- 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.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

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. Records will be supplied within 21 working days of receipt of a written request.

11. Photographs and videos

As part of our Pre-School activities, we may take photographs and record images of individuals within our Pre-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 Pre-School on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of Pre-School by external agencies such as the school photographer, newspapers, campaigns.
- Online on our Pre-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.

12. 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 DPO, and ensuring they have the necessary resources to fulfil their duties.
- 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)
- 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.

13. 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 in a secure location when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.

- Where personal information needs to be taken off site it must be securely stored and returned as soon as possible.
- Passwords that promote additional security (random words, numbers and special characters) are used to access documents and systems containing personal information.
- 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 (see section 8).

14. 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.

15. Personal data breaches

The Pre-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 a set procedure and make a report to the ICO within 72 hours. Such breaches in a Pre-School context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

16. Training

All staff and trustees are provided with data protection training. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Pre-School's processes make it necessary.

17. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.