The Froebelian School
Data Protection Policy

The provisions in this document apply to all aspects of the school including First Steps nursery, the EYFS, Breakfast Club, Little Acorns, Homework and Activities Club, Summer Holiday Club, school trips and extra-curricular activities.

Rationale for the Policy
This policy has been created to ensure that The Froebelian School meets its data protection obligations, including new General Data Protection Regulations, whilst adhering to statutory requirements already existing within the education sector.

Policy aim
To provide guidance for staff, parents and the wider community in fulfilling GDPR requirements.

Introduction

This policy sets out the school's commitment to data protection and individual rights and obligations in relation to personal data. As part of its normal day-to-day operations, the School holds and processes relevant personal data regarding employees, parents, students, alumni, students applying for admission and their parents, agents, and friends. The principles of GDPR shall be applied to all data processed by the school. The Froebelian School commits to:

- Ensure that data is fairly and lawfully processed;
- Process data only for defined and legitimate purposes;
- Ensure that all data processed is adequate, relevant and not limited in relation to the purpose;
- Ensure that data processed is accurate;
- Not keep data longer than is necessary;
- Process data in accordance with the data subject's rights;
- Ensure that data is secure;
- Ensure that data is not transferred to outside agencies without adequate protection.

The school regularly reviews all manual and electronic files to ensure compliance with these principles; to ensure security and integrity of filing systems; and to ensure that access to them is only available to an authorised person(s).

Related and connected laws:

- The General Data Protection Regulations 2016;
- The Common Law Duty of Confidentiality;
- The Freedom of Information Act 2000;
- Privacy and Electronic Communications Regulations 2003;

- Computer Misuse Act 1990;
- Human Rights Act 1998.

General Principles and Scope

The Froebelian School is committed to the protection of all personal and special categories of personal data for which it holds responsibility as the Data Controller, and the handling of such data in line with data protection principles and GDPR legislation. Any changes to this legislation will be monitored and implemented in order to remain compliant with all requirements. Employees of the school will receive regular notifications and training so as to ensure on-going awareness and compliance in line with GDPR requirements.

In accordance with regulatory requirements, the school has notified the Information Commissioner's Office of its processing activities. The school's ICO registration number is Z8545786 and its registered address is: The Froebelian School, Clarence Road, Horsforth, Leeds LS18 4LB.

The requirements of this policy are mandatory for all staff, volunteers and casual or supply workers employed by the school and any third party contracted to provide services within the school.

Terms and Abbreviations

- **GDPR – The General Data Protection Regulation** is a regulation by which the European Parliament, the Council of the European Union and the European Commission seek to strengthen and unify data protection for all individuals within the European Union. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. GDPR comes into force on 25 May 2018.
- **ICO – Information Commissioner's Office**. The Information Commissioner is an independent official appointed by the Crown. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal. The Office's mission is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals."
- **Personal Data** – means any information relating to an identified or identifiable natural person (living) ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Special Categories of Personal Data –** means any sensitive personal data relating to race, ethnic origin, political opinions, religion, philosophical beliefs, trade union membership, genetic data, biometric data, health data, data concerning a natural person's sex life, sexual orientation.
- **DSAR – Data Subject Access Request** is the process by which an individual (data subject) can request access to data about them held by the school (*see section 7*).
- **Data Controller, in our case, the School** - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Data Processor** - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Data subject, in our case Data subjects are staff members, pupils, parents, etc.**;
- **Data Process Owner** - the person responsible for the instigation or on-going maintenance of a data process or data processing operation;

- **Identifiable living individual** - means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, phone number or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;
- **Processing** - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Personal Data Breach** - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, for example, sending email to the wrong recipient, a disciplinay file may be stolen and so on;
- **Risk** - the risk to the loss of, or unauthorised sharing of personal data.. It is measured in terms of consequence and likelihood;
- **Risk Management** - the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;
- **Recipient** - means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. **Third party** - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- **Consent** - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;
- **'The school' –** refers to The Froebelian School unless otherwise stated

1. Roles & Responsibilities

1.1. The governing body has overall responsibility for ensuring that the school complies with its obligations under the Data Protection act and GDPR.

1.2. Day to day responsibility lies with the Headteacher, delegated to the Finance & Operations Manager, who is the school's allocated Privacy Officer.

1.3. The Privacy Officer is responsible for ensuring that staff are regularly trained and aware of their data protection obligations, and will oversee any queries related to the storing or processing of personal data.

1.4. As a small business, we are not required to have a Data Protection Officer.

1.5. Individual staff members are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their own personal data, such as a change of address.

2. Lawful Processing of Personal Data & Consent

2.1. The Froebelian School processes some data under Article 6 EU GDPR "Lawfulness of processing", section (f). To process personal data for pupils we rely on consent, contractual obligations and performance of a public function.

2.2. Data subjects provide the school with their personal data at various contact points and at various points in time from applications to enter school through to alumni events.

2.3. Data subjects of the school are mostly limited to those who have a specific interest in The Froebelian School as a pupil, parent, staff member, alumni or friend of the school.

2.4. Lawful processing of data is necessary in performing our contractual and legal obligations to our pupils, their parents/guardians and employees. The school publishes a Privacy Notice to ensure transparency about the intended processing of data..

2.5. In the case of current pupils and their parents or guardians, lawful processing of personal data is necessary in the performance of the school's core duty to support teaching and learning; take appropriate physical and pastoral care of the child and to assess how the school is performing (including provision of information to the Department for Education or other regulatory or inspection bodies); and in order to meet our contractual and legal obligations to the pupil, parent or guardian. In all such cases, explicit consent for data processing beyond the parental contract is not required and will not be sought, regardless of the age of the child.

2.6. Personal data processed lawfully for the school's core educational purposes will include (but not be limited to) current and prospective pupil and parental contact and identification details; results of internal and externally set tests and assessments (including school grades and reports); data on pupil characteristics (such as ethnic grouping or special educational needs); exclusion information; details of medical conditions; safeguarding and child protection information.

2.7. In the case of current or prospective staff, volunteers and other workers, lawful processing of personal data is necessary in the performance of the school's role as an employer; and in order to meet contractual and legal obligations. In all such cases, explicit consent for data processing is not required and will not be sought.

2.8. Personal data processed lawfully for core employment purposes will include (but not be limited to) staff contact and identification details; national insurance numbers; contract and salary information; qualifications; absence data; staff personal characteristics, equality and medical information; outcomes of any disciplinary procedures. Such data will be used to assist with the running of the school, including to enable individuals to be paid; to facilitate a safe working environment; to support the effective performance management of staff; to improve the management of workforce data across the sector; to inform our recruitment and retention protocols; to allow for financial modelling and planning; to enable ethnicity and disability monitoring; and to support the work of senior leadership and the governing body in implementing operational and strategic plans.

2.9. In general, the school will assume that pupils consent to disclosure of lawfully processed personal data to their parents or guardians regardless of age unless, in the school's opinion, there is a good reason to do otherwise (such as the specific withdrawal of this consent by the child; a legal process preventing sharing of data; or a safeguarding concern).

2.10. Where the school seeks to use currently held data for a purpose other than that for which it was originally intended, or seeks to obtain data for an activity which does not fall under contractual or lawful processing purposes, consent will be obtained in advance. No personal data will be used for any purpose other than that which it was collected and/or created for without the approval of the Privacy Officer.

2.11. The Froebelian School will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collects.

Data process owners are responsible for ensuring that no unnecessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The Privacy Officer will provide advice regarding the justification of personal data collected or created.

2.12. The Froebelian School recognises that the accuracy of data is important and that some data is more important to keep up-to-date than others. The organisation will use its reasonable endeavours to maintain data is as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date. Data process owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained as accurate and up-to-date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up-to-date are treated appropriately through erasure or anonymisation. The Privacy Officer will provide advice regarding data accuracy.

2.13. Consent must be a freely given (giving due consideration to imbalances of power between the data subject and the school), specific, informed and unambiguous indication of the individual's wishes, and will take the form of a clear affirmative action. The school will never assume consent has been given through inaction or a non-response.

2.14. Where consent is required for the processing of personal data about a child, it is recognised that this data belongs to the child and not to the child's parents or guardians. Following ICO guidance, consent for processing personal data of a child aged 13 or older must be obtained directly from the child. For younger children parents may grant consent on their behalf, following appropriate checks to ensure that they hold legal responsibility for the child.

2.15. Privacy notices for children will be written using clear and age-appropriate language.

2.16. In seeking to obtain consent, the school will comply with GDPR requirements that the consent form will be separate from other forms or terms and conditions, and will provide clear information including instructions on how to withdraw consent at a later date.

2.17. The Froebelian School has put in place measures to ensure that the rights and freedoms of its data subjects are not unduly harmed by its data processing. The school has written and published its full Privacy Notice and related data protection policies. These policies further document in detail the types of data collected, the processing undertaken by the school and the rights of the data subjects.

3. Data Handling & Security

3.1. All staff members are responsible for ensuring that reasonable measures are in place to protect personal data and prevent its loss and unauthorised or unnecessary dissemination. This means that staff will ensure that any personal data they hold is kept securely, and that it is not disclosed either orally or in writing or otherwise to any unauthorised third party without the data subject's explicit permission.

3.2. Paper-based records and portable electronic devices, such as laptops and hard drives which contain personal data are kept under lock and key when not in use, and the creation of unnecessary paper copies of personal data is to be avoided.

3.3. Papers containing confidential personal information should not be left on office or classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

3.4. Where personal information needs to be taken off site (in paper or electronic form) staff will ensure that suitable steps are taken to ensure that it is kept safe and secure, and not accessible to anybody who is not entitled to have access to it.

3.5. Passwords used to access school computers, laptops and other electronic devices are required to fulfil the requirements of the School's Password Policy.

3.6. Encryption software and/or password protection is used to protect all portable devices and removable media, such as laptops and USB devices.

3.7. Staff, pupils or governors who store personal data on their personal devices are expected to follow the same security procedures as for school owned devices.

3.8. To fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation as well as in support the policy on transparency, The Froebelian School will maintain records of the processing activities that it controls, undertakes or otherwise commissions as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR.

4. Data Sharing

4.1. The school has a number of contracts with third party organisations which assist with the delivery of educational and employment functions at The Froebelian School. In such cases, personal data of current or prospective staff and/or pupils is sometimes shared by the school with these parties to allow for the fulfilment of contractual obligations and/or business efficiency and effectiveness.

4.2. Additionally, the school is sometimes required by law or in the best interests of the pupils or staff to share information with external authorities (such as the local authority, Independent Schools' Inspectorate, or the Department for Education).

4.3. Where data is shared with a third party organisation, only the data necessary for the completion of the contract or legal obligation is provided by the School, and risk assessments, formal contracts and/or agreements are sought which commit third party organisations to the same standards of data protection as apply to the school. A register of these agreements is maintained by the Privacy Officer.

4.4. Where formal agreements cannot be obtained from third party organisations seeking data held by the school, then consent to share data will be obtained in advance from the data subject.

4.5. The Froebelian School reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. People wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The Privacy Officer will provide advice and guidance in respect of this. A written agreement will be implemented between the organisation and the data processor which at least

meets the requirements of the Data Protection Legislation. The Privacy Officer will ensure that a register of such agreements/arrangements is maintained. The data processor agreement will specify what is to happen to personal data upon termination of the data processing agreement. No employee is permitted to commission or appoint a third party to process personal data on behalf of The Froebelian School without adhering to this policy.

4.6. The Froebelian School will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined. Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the Privacy Officer and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has an adequacy decision issued by the European Commission;
- The transfer is to the United States of America and the recipient is registered under the EU/US Privacy Shield scheme;
- The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

5. Data Retention and Disposal

5.1. Personal data that is no longer needed by the school or an individual member of staff in fulfilment of their role (except in cases where there is a statutory or legal reason for it to be retained), or else has become inaccurate or out of date, is disposed of securely. It is recognised that data will be retained for different lengths of time, according to the needs and obligations of the school.

5.2. Paper based personal data which needs to be disposed of should be placed in one of the secure, locked shredding bins provided in locations throughout the school. All materials placed in these containers will be shredded.

5.3. Electronic personal data that is no longer needed should be deleted from all local, cloud based or online storage locations. Staff are expected to 'double delete' all such records to ensure that they are fully removed from devices and all storage locations.

5.4. Emails containing personal data should similarly be 'double deleted' when they are no longer needed.

5.5. Detailed guidance to staff on the statutory and/or recommended retention periods of different pieces of personal data are contained within the Data Retention Policy.

However, it is recognised that not every eventuality can be outlined in such a policy, and staff are expected to use their professional judgement on whether data they hold (other than in cases with statutory retention periods) remains necessary to the running of the school or their role within the school.

6. Data Subject Rights (logging objections; right to be forgotten, data quality maintenance)

6.1. All data subjects have rights in relation to the collection, storage and processing of their personal data.

6.2. Data subjects have a right to request that inaccurate information about them is erased or corrected, and may do so by contacting the Privacy Officer in writing.

6.3. Data subjects have a right to withdraw their consent for the processing of their data (other than where this is lawfully processed in the performance of the school's contractual or legal obligations), and may do so by contacting the Privacy Officer in writing.

6.4. Data subjects have a right to data erasure (the 'right to be forgotten') where their personal data is not required for an on-going contractual or educational obligation within the bounds of lawful processing. Data subjects can invoke this right by contacting the Privacy Officer in writing. Data subjects should be aware that some personal information must be retained to allow the School to comply with the request (e.g. to enable contact to be maintained during the processing of the request).

6.5. Data subjects have the right to a 'Data Subject Access Request' (see section 7).

7. Data Subject Access Requests

7.1. Data subjects have a legal right to request access to information the school holds about them, subject to certain exemptions and limitations set out under GDPR, or where safeguarding concerns or legal processes preclude the sharing of data. This is known as a Data Subject Access Request.

7.2. Data Subject Access Requests should be directed to The Froebelian School's Privacy Officer. Requests should include the name of the data subject about whom the request is being made; a correspondence address; a contact number and email address and details about the specific information requested.

7.3. All Data Subject Access Requests will be responded to within one month providing all the necessary information to process the request has been received, and no charge will be applied to process the request. If there is a reason why a DSAR cannot be completed within the allocated time, then this will be communicated in writing to the person making the request prior to the originally scheduled date of completion. Where the school decides to decline a DSAR, this will be communicated in writing to the person making the request, outlining where legally possible the reasons for refusing the request.

7.4. Following ICO guidance, only children aged 13 or above are considered able to understand their rights with regards to data protection and Data Subject Access Requests. Therefore, any DSAR for a child under this age must come from the parent who may make a request on behalf of the child.

7.5. Data Subject Access Requests do not give the data subject any rights to obtain data on other individuals, and therefore any information provided in response to a DSAR will be suitably redacted to prevent identification of individuals through third party data.

8. Data Protection Breaches and Notifications

8.1. The Froebelian School takes seriously any potential breaches of its duty to protect personal data.

8.2. If the school, a data processor or a data subject believes that the school has not complied with this policy or acted otherwise than in accordance with the General Data Protection Regulations, they should in the first instance inform the school's Privacy Officer in writing, either by letter or email.

8.3. The Privacy Officer will always investigate possible data breaches, and the school is committed to reflecting upon and developing its practice, policies, training or staff awareness in response to any detected breaches. A record of 'near misses' and breaches, along with outcomes from subsequent investigations is kept by the Privacy Officer.

8.4. Under GDPR, the school is required to notify the ICO of any data breaches within 72 hours of becoming aware of them, if this incident resulted in a privacy breach to the affected individuals. Failure to do so can result in a fine. XX

8.5. If an individual believes that the Privacy Officer has not responded to their notification of a breach appropriately, then they should pursue this through the school's complaints procedure.

9. Risk Assessment

9.1. The Froebelian School will embrace the principles and foster a culture of privacy by design and by default. It will maintain a policy requiring data protection impact assessments (DPIA) to be undertaken when commencing a new project which will involve the capture or processing of personal data, or with an existing process when the school intends to change the way personal data will be used or processed. The Privacy Officer is responsible for maintaining a risk register of data protection compliance risks that have been identified by the organisation and for its periodic review.

10. Training and Awareness

10.1. The Froebelian School will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

11. Audit and Compliance Checking

11.1. The Froebelian School will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where non-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Governing Body will be provided with a summary of audit findings periodically.

Further information about GDPR and Data Protection can be obtained via:

The Froebelian School's Privacy Officer

Tineke Roth – Finance & Operations Manager

The Froebelian School
Clarence Road
Horsforth
Leeds
LS18 4LB
t.roth@froebelian.co.uk

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
https://ico.org.uk/

This policy is reviewed regularly by the Headteacher, in consultation with the governing body, in the light of experience, research and good practice.

Policy Date:	May 2018
Policy Review Date:	May 2021
Signed (Headteacher):	
Signed (Chair of Governors):