The Firs Lower School

GDPR Policy

1. Statement of intent

The Firs Lower School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies such as the DfE, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school handles data to comply with the following core principles of the GDPR (See section 4)

Through this policy The Firs Lower School sets out how it will keep data secure and outline the importance that all data is treated in accordance with the new regulations. This policy will be backed up by protocols and other policies including:

- Acceptable Use and E Safety Policy
- Firs GDPR Information Audit - appendix 1
- Privacy Notice - GDPR appendix 2
- Freedom of Information publication scheme protocol - GDPR appendix 3
- Retention of data Schedule - GDPR appendix 4 (Google Sheet)

2. Legal framework

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)

The Freedom of Information Act 2000

The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

- The School Standards and Framework Act 1998

This policy has also considered the following guidance:

Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'

Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3. The policy will apply to:

People The policy applies to all school staff, governors (Members and Trustees) parents/carers, pupils and others in so far as the measures under the policy relate to them.

Data This means information in a form that can be processed. It includes automated data (information that is on a computer or information recorded with the intention of putting it on to a computer) and manual data (information that is kept as part of a relevant filing system)

Relevant filing system means any set of information, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information relating to an individual is readily accessible.

Personal data means data relating to a living individual who is or can be identified from the data or from the data in conjunction with other information that is or is likely to come into possession of the data controller

Data Controller (DC) A data controller is an individual or legal entity which controls the content and use of personal data. The school has a number of data controllers (principally SLT members and the ICT administrator)

Data Protection Responsible Officer (DPRO) - the Headteacher will take the role of the DPRO, ensuring compliance with this policy and the GDPR

4. Principles

In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- The GDPR also requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”.

5. Accountability

The Firs Lower School will implement appropriate measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The school will provide comprehensive, clear and transparent privacy notices. (See Appendix 2)

Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

6. Data protection officer (DPO)

A DPO will be appointed in order to:

- Inform and advise the school including the Data Controllers and DPRO and all the staff and Governors about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school’s compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.
- An outside body / individual or existing employee will be appointed to the role of DPO. Where an existing member of staff is appointed, the Governors need to be confident that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.
- The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
- The DPO will report to the DPRO and the F and E Committee of the Governors, often liaising with the School Business Manager (one of the school’s DCs)
- The DPO will operate independently and will not be dismissed or penalised for performing their task.
- Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

7. Fair and Lawful processing

The school holds information on pupils and in doing so, have to follow the Data Protection and related Acts. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. The school has a Privacy Notice which explains how personal data is used and with whom it will be shared. This Notice is published on the school website.

a. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.

- Processing is necessary for:
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

b. Processing of data at The Firs and The Saplings Pre School will follow the following stipulations:

- Personal data and school records about pupils are confidential to the child. The information can be shared appropriately within the professional working of the school to enable the school to make the best educational provision for the child. The law permits such information to be shared with other educational establishments when pupils change schools.
- The retention periods for different types of information are set out in the Retention protocol Appendix 4.
- All members of staff should only access school-provided systems (including e-mail) up to the last day of employment.

(For further information see the Retention of Data Protocol - Appendix 4)

8. Consent

- Consent must be a positive indication e.g.‘opt in’ not ‘opt out’.
- Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual’s wishes.
- Where consent is given, a record will be kept documenting how and when consent was given.
- The school ensures that consent mechanisms meet the standards of the GDPR.
- Consent can be withdrawn by the individual at any time.

9. The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the data controller
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the data controller or third party.

- Any recipient or categories of recipients of the personal data.
- Details of transfers to third parties and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.
- For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- In relation to data that is not obtained directly from the data subject, this information will be supplied
    - Within one month of having obtained the data.
    - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
    - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access and SARs

- Individuals have the right to submit a **subject access request** (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
- The school will verify the identity of the person making the request before any information is supplied.
- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on the administrative cost of providing the information.
- All requests will be responded to without delay and at the latest, **within one month of receipt.**
- In the event of numerous or complex requests, the period of compliance will be extended by a further **two months**. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, **within one month of the refusal**.
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

11. The right to rectification

- Individuals are entitled to have any inaccurate or incomplete personal data rectified.
- Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- Requests for rectification will be responded to **within one month**; this will be extended by two months where the request for rectification is complex.
- Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12 The right to erasure

- Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- Individuals have the right to erasure in the following circumstances:
    - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
    - When the individual withdraws their consent (this cannot apply to data which the school collects legally (in compliance with GDPR as part of his normal function)
    - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - The personal data was unlawfully processed
    - The personal data is required to be erased in order to comply with a legal obligation
    - The personal data is processed in relation to the offer of information society services to a child

- The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:
- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority (e.g. child protection or to pass data to DfE as part of the school's statutory duty)
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.
- Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

- Individuals have the right to block or suppress the school's processing of personal data.
- In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.
- The school will restrict the processing of personal data in the following circumstances:
    - Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
    - Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
    - Where processing is unlawful and the individual opposes erasure and requests restriction instead
    - Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
- If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.
- The school will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.
- The right to data portability only applies in the following cases:
- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

- Personal data will be provided in a structured, commonly used and machine-readable form.
- The school will provide the information free of charge.
- Where feasible, data will be transmitted directly to another organisation at the request of the individual.
- **The Firs Lower school** is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.
- The school will respond to any requests for portability **within one month**.
- Where the request is complex, or a number of requests have been received, the time frame can be extended by **two months**, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

- Where no action is being taken in response to a request, the school will, without delay and at the latest within **one month**, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

- The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.
- Individuals have the right to object to the following:
    - Processing based on legitimate interests or the performance of a task in the public interest
    - Direct marketing

- Where personal data is processed for the performance of a legal task or legitimate interests:
    - An individual's grounds for objecting must relate to his or her particular situation.
    - The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

- Where the processing of personal data is necessary for the performance of a public interest task e.g. to assess children against the National Curriculum, the school is not required to comply with an objection to the processing of the data.

16. Data protection impact assessments (DPIA)

The school will act in accordance with the GDPR by implementing measures that show that the school has considered and integrated data protection into all data processing activities.

- Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.
- A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.
- A DPIA will be used for more than one project, where necessary.
- Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. Data breaches

- The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

- The **Headteacher as Responsible Officer** will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.
- Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.
- All notifiable breaches will be reported to the relevant supervisory authority **within 72 hours** of the school becoming aware of it.
- The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
- In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.
- A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
- In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
- Within a breach notification, the following information will be outlined:
    - The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
    - The name and contact details of the DPO
    - An explanation of the likely consequences of the personal data breach
    - A description of the proposed measures to be taken to deal with the personal data breach
    - Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

18. Data security

- Confidential paper records will be kept in a locked filing cabinet, drawer or similar, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Paper based SEND records will be kept in the Swallow Room, where both doors are protected by code entry systems. Any online systems storing individual data, such as Tapestry, will be asked to provide statements that they are GDPR compliant.
- Other digitally stored data will be kept on the Google Drive protected by two factor authentication.
- Data will **not** be saved onto individual machines, removable storage or a portable devices such as memory sticks.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock

and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

- Before sharing data, all staff members will ensure:

  -They are allowed to share it.

  -That adequate security is in place to protect it.

  -Who will receive the data has been outlined in a privacy notice.

- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a **termly** basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The **Data Protection Officer** is responsible for continuity and recovery measures are in place to ensure the security of protected data

(See Information Audit - Appendix 1 and Privacy Notice - Appendix 2)

19. Publication of information

The Firs Lower School makes the following information routinely available on its website :

- School or college contact details
- Admission arrangements
- Exclusion arrangements (Part of Behaviour Policy)
- Ofsted reports
- Curriculum overview and Scheme of Work (science and foundation subjects)
- Key policies including Child Protection, Behaviour, Equality (incorporating Equality Objectives), SEND, Charging and Remissions and Complaints
- Pupil premium annual plan / review
- Sport premium annual plan / review
- Special educational needs and disabilities (SEND)
- Financial records
- Governors' information and duties including the annual report.
- Values and ethos

Classes of information specified in the publication scheme are made available quickly and easily on request. (See appendix 3)

The School will not publish any personal information, including photos, on its website without the permission of the affected individual.

20. Video and Photography

- The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

- The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- 'Opt in' permission for the taking of photos or videos will be obtained when each pupil joins the school. A record of which pupils **do not** have this permission will be kept in a secure Google Document on the 'Pupil Information and Parent Meeting Drive'.
- Images captured by individuals for recreational/personal purposes, and videos made by parents **for family use**, are exempt from the GDPR.

21. Data retention

- Data will not be kept for longer than is necessary.
- Unrequired data will be deleted as soon as practicable.
- Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
- Paper documents will be shredded / placed in Confidential Waste bags and electronic copies deleted, once the data should no longer be retained. (See Retention of Data Protocol - Appendix 4)

22. DBS data

- All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
- Data provided by the DBS will never be duplicated.
- Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

Policy review

This policy is reviewed every **2 years** by the **Headteacher as DPRO and the F and E Committee**