Mapplewells Primary & Nursery School

Data Protection Policy

Approved by:	Mapplewells Primary Governing Body	**Date:**	
Last reviewed on:	September 2023		
Next review due by:	September 2024		

Contents

1. Aims

Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

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

The Flying High Partnership and schools within the multi academy group are 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 Trust/school may, from time to time, be required to share personal information about its staff or pupils with other organisations, such as local authorities, the Department for Education, other trust schools and educational bodies, and potentially external agencies.

This policy is in place to ensure all staff, Trustees and governors are aware of their responsibilities and outlines how the school complies with the core principles of the GDPR.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Act 1998, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

It also takes into account the provisions of the General Data Protection Regulation, which is new legislation effective as of 25 May 2018.

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. This policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The data controller

Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller. Our school delegates the responsibility of data controller to the Office Manager

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data protection principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the Data Protection Act 1998.

Day-to-day responsibilities rest with the headteacher, or the deputy headteacher in the headteacher's absence. The headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff 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 personal data, such as a change of address.

7. Data Protection Officer (DPO)

The DPO role will work with the Operations Manager, Director of Business and Finance Director and HR Manager to:

- Inform and advise schools and its employees 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.
- Day-to-day responsibilities rest with the headteacher, or the local data protection representative who will be the Office Manager or School Business in the headteacher's absence. The headteacher will assist the DPO in ensuring that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.
- Staff 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 personal data, such as a change of address

- The DPO will report to the highest level of management of the trust, which is the Board of Trustees.

8. Privacy/fair processing notice

8.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 9 and 10 of this policy.

We are required, by law, to pass certain information about pupils to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

8.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Office Manager

9. Subject access requests

Under the Data Protection Act 1998, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. . Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

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

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The table below summarises the charges that apply.

Number of pages of information to be supplied	Maximum fee (£)
1-19	1.00
20-29	2.00
30-39	3.00
40-49	4.00
50-59	5.00
60-69	6.00
70-79	7.00
80-89	8.00

90-99	9.00
100-149	10.00
150-199	15.00
200-249	20.00
250-299	25.00
300-349	30.00
350-399	35.00
400-449	40.00
450-499	45.00
500+	50.00

If a subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply is £10.00.

10. Parental requests to see the educational record

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

11. Storage of records

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- 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 for school-owned equipment

- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

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.

12. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records. A disposal log is maintained by the school office and disposal is in line with the retention guidelines for specific records and documentation. Refer to the Trust retention schedule for guidance and ensure all documentation or records (electronic or paper based) are added to the disposal log.

13. Data Breaches

On occasion data may be compromised or shared accidentally and in contravention of the Data Protection Policy. In the first instance the breach should be reported to the Trust via Nick Layfield, nlayfield@flyinghightrust.co.uk or 0115 9891915. At this stage further guidance will be provided as to whether the breach is to be reported to the ICO and/or recorded on the school Data Breach Log. Any remedial actions, including notifying data subjects of the breach, will be agreed and documented on the Data Breach Log.

- 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.
- 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 trust will notify those concerned directly.
- 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 throughout the trust, 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 and other key personnel who may give support
- 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

14. Training

Our 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 or the school's processes make it necessary.

15. The General Data Protection Regulation

We acknowledge that the law is changing on the rights of data subjects and that the General Data Protection Regulation is due to come into force in May 2018.

We will review working practices on an ongoing basis and provide training to members of staff and governors where appropriate.

16. Monitoring arrangements

The Trust Operations Manager is responsible for monitoring and reviewing this policy at Trust level. [Insert role – Headteacher or SBM] is responsible for ensuring the content relevant to our school is reviewed and updated.

The Trust Operations Manager and Trust Data Protection Officer check that the school complies with this policy by, among other things, reviewing school records on an annual basis.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every 2 years**.

At every review, the policy will be shared with the governing body and the updated policy made available via the school website and copies available on request from the school office.

17. Links with other policies

This data protection policy and privacy notice is linked to the freedom of information publication scheme. Refer also to the Trust and schools Privacy Notice and Retention Schedule, Breach Reporting Log and Personal Data Disposal Log.