MEREBROOK INFANT SCHOOL

GENERAL DATA PROTECTION (GDPR) POLICY

VERSION

Date	Author(s)	Notes on Revision/s
November 2018	Tracy Hurwood	New Policy
Policy Review: Every 2 years **Type of Governing Board Meeting:** Full Governing Board Meeting		

Table of Contents

This policy applies to all staff, parents and pupils of the school and anyone with whom the school has a relationship or may have need to contact. The General Data Protection Regulation (GDPR) came into force on 25 May 2018.

This policy sets out the school's commitment to protecting the rights and freedoms of data subjects and the safe and secure processing of their data in accordance with our legal obligations. This policy describes how the school collects, handles and processes, stores and deletes this data.

1 DEFINITIONS

Data Controller

The entity which decides how and why and under what conditions personal data are processed.

Data Processor

This is the person who processes the data on behalf of the data controller. This is a school employee with specified responsibilities.

Data Protection Officer (DPO)

The person who is responsible for ensuring that the school adheres to the GDPR principles. The school contracts this position to an independent body.

Data Subject

A living person to whom the personal data relates.

Personal Data

This includes everything from which a data subject can be identified, such as name, physical address, email address, identification number and health records. Personal data can include expressions of opinion about that individual, file notes or minutes and communications (such as email) with or about them

Sensitive Personal Data

Some categories of data are 'special category data' under the GDPR, broadly equivalent to 'sensitive personal data'. This includes information about the individual's race, ethnicity, political opinions, religion, trade union status, health, gender, sexual orientation and criminal record. Such information is treated with particular care. Financial data is also treated as 'sensitive personal data'. Processing this means obtaining, recording or holding data or carrying out any operation on it, including its retrieval, consultation or use.

2 GENERAL STATEMENT OF THE SCHOOL'S DUTIES

The school is required to gather and use certain information about individuals, including staff, children, parents and others with whom the school has a relationship or may need to contact.

The school will ensure that all staff who have responsibility for processing data are aware of the contents of this policy and the conditions under which data should be processed. The

school will also inform those about whom it holds data, the conditions for processing, in the form of a Privacy Notice.

This policy sets out how the school seeks to ensure that employees understand the rules governing the use of personal data to which they have access in the course of their work.

This policy requires staff to ensure that the DPO is consulted before any significant new data processing activity is initiated to ensure that the school is always compliant with its legal obligations.

3 LAWFUL BASIS FOR WHICH THE SCHOOL PROCESSES DATA

The school processes data for the following reasons:

1. **Contractual.**
   For example, parents enter into a contract with the school to provide education to children and employees enter into an employment contract with the school.
2. **Compliance with a legal obligation.**
   The school is obligated to process data to meet UK and EU law.
3. **Vital interests.**
   The school can process data if it's necessary to protect someone's health and/or life. This could be the life of the data subject or someone else. This will mean that the school obtains and processes data relating to health and emergency contacts.
4. **Lawful function of a public body.**
   The school will process data to perform its official tasks.
5. **Legitimate interests.**
   The school can process personal data without consent to meet the legitimate interests of providing an education to children. The school will ensure it is fair, transparent and accountable.
6. **Consent.**
   The school holds clear and defined consent for the individual's data to be processed for a specific purpose, for example, the use of photographs.

3.1 EIGHT PRINCIPLES

The school understands its responsibilities to fully adhere to the principles of data protection, contained within the GDPR, which specify that the data must be:

1. Fairly and lawfully processed.
2. Processed for limited purposes.
3. Used in a way that is adequate, relevant and not excessive.
4. Accurate.
5. Not kept for longer than necessary.
6. Processed in line with the individual's data protection rights.
7. Kept secure and safe.
8. Not transferred to countries outside the European Economic Area (EEA) without adequate protection.

3.2 RIGHTS OF INDIVIDUALS

The school recognises the following rights of individuals:

The **Right to be Informed** about the processing of their personal data.

The **Right of Access** to their personal data and supplementary information and the right to confirmation that their personal data is being processed.

The **Right to Rectification** if their personal data is inaccurate or incomplete. Where an individual wishes to make amendments, the DPO should be informed. Requests to amend data will normally be processed within 28 days.

The **Right to be Forgotten.** Where there is no compelling reason for the school to continue to process the data, the data will be deleted or securely destroyed.

The **Right to Restrict Processing** of their personal data, for example, if they consider that the processing is unlawful or the data is inaccurate.

The **Right to Portability** of their personal data for their own purposes. Data subjects will be allowed to obtain and reuse their data for their own purposes. A data subject can request that their data is transferred directly to another system. This must be done without charge.

The **Right to Object** to processing of their personal data for such purposes as marketing or statistical analysis.

3.3 EXEMPTIONS

There are a number of exemptions where information may be withheld, for example, to do with safeguarding and information sharing protocols relating to child protection actions. The school will always comply with its statutory and regulatory obligations.

4 SUBJECT ACCESS REQUESTS (SAR)

This is also known as the Right to Access. It entitles the individual to have access to and information about the personal data that the data controller has about them.

A SAR should be made to the DPO. A SAR should be made in writing. However, the school will accept such requests by letter or email. The school must verify the identity of the person making the request. The DPO is responsible for organising the response to the SAR and the information will be supplied to the requestor within 28 days of receiving the SAR, free of charge.

In circumstances where the request is complex, the deadline can be extended by a further two months. If this is the case, then the DPO will inform the requestor within one month of receipt of the request, explaining why the extension is necessary. The information will be supplied to the requestor within two months from the end of the first 28-day period. The DPO must approve any extension.

The school may refuse to respond to certain requests and in such cases, an explanation will be supplied to the requestor.

In circumstances of the request being manifestly unfounded or excessive and/or repetitive, the school may charge a reasonable fee to cover the administrative costs. Approval from the DPO is required in such an instance. The information will be supplied in a commonly used electronic format.

5 STORING DATA SECURELY

- The following guidelines are in place and all staff are expected to adhere to these expectations:
- Where information is stored on printed paper, it will be kept securely in a place where unauthorised personnel cannot access it.
- Printed data will be shredded when it is no longer needed.
- Data stored on computers and tablets will be stored with strong passwords.
- Data will only be shared by email using an approved secure encrypted system.
- Data stored on memory sticks must be encrypted and stored securely when not in use.
- Where a cloud is used to store data, then such usage will be authorised by the DPO.
- Servers containing personal data will be kept in a secure location. Servers will be protected by security software and strong firewalls.
- Data will be regularly backed up in line with school procedures.
- Data will only be stored on approved secure devices.
- Archived data will be stored securely and kept only for as long as necessary. We follow the Information and Records Management Society's (IRMS) guidance on information retention for schools. There are different retention periods for different types of school records and we follow the guidance in the table on pages 37-56 of the IRMS toolkit for schools. This can be found at:

https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

5.1 TRANSFERRING DATA INTERNATIONALLY

There are restrictions on international transfers of personal data. Each circumstance will be reviewed individually and data processors must not transfer any data outside of the UK without the authorisation of the DPO. Specific consent from the individual must be obtained prior to the data transfer.

5.2 CRIMINAL RECORD CHECKS

These are considered to be sensitive personal data. As part of the school's Safer Recruitment practices, criminal records checks are undertaken for staff with the Disclosure and Barring Service (DBS).

5.3 INFORMATION ASSET REGISTER

The school will maintain an up-to-date Information Asset Register to demonstrate compliance. This contains information on what data is held, the lawful basis on which it is held, where data is stored, how it is used, who is responsible for the data and information about retention timescales. The Information Asset Register will be audited annually by the DPO.

5.4 DATA BREACHES

Data processors must inform the DPO of any breach immediately. Serious breaches of data must be notified to the ICO within 72 hours. The DPO will maintain an internal record of any data breaches.