



# Longmoor Community Primary School Data Protection Policy

## Introduction

On the 25th May 2018 the General Data Protection Regulation (GDPR) will be applicable and the current Data Protection Act (DPA) will be updated by the new Act giving effect to its provisions. Before that time the provisions of the DPA 1998 will continue to apply.

The policy sets out the manner in which personal data of staff, pupils and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, pupils, parents or carers and other individuals who come into contact with the School. The information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the School complies with its statutory obligations.

The School is a Data Controller and is registered with the 'Information Commissioner's Office' (ICO) and must therefore demonstrate compliance with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, protected, disclosed and securely disposed of.

## Aims

The Policy aims to ensure that:

- The School processes all personal data fairly, lawfully and transparently in compliance with the Data Protection Principles.
- All staff involved with the collection, handling, processing and disclosing of personal data will be aware of their duties and responsibilities.
- The data protection rights of those involved with the School Community are safeguarded.
- Everyone can have confidence in the School's ability to process data fairly and securely.

## Scope

This Policy applies to:

- Personal data of all School employees, governors, pupils, parents and carers, volunteers and any other person carrying out activities on behalf of the School.
- The processing of all data whether in manual or electronic form.
- All Governors, Staff and Contractors.

## The Data Protection Principles

The School will ensure that personal data will be:

- 1) Processed fairly, lawfully and in a transparent manner.
- 2) Collected for specified, explicit and legitimate purposes.
- 3) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- 4) Accurate and, where necessary, kept up to date.
- 5) Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data it is processed.
- 6) Processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The School will be able to demonstrate compliance with these principles.

The School will also have in place a process for dealing with the exercise of the following rights by Governors, Staff, Pupils, Parents and members of the public in respect of their personal data by providing on lawful request:

- Details of what personal data is held, why it is being processed and who it is shared with.
- Access to their data.
- Correction of inaccuracies.
- Erasure, where the holding of that data is not a statutory or legal requirement.
- To restrict processing, where the holding of that data is not a statutory or legal requirement.

There exists further rights to the following:

- Data portability.
- Objection to processing.
- Not to be subject to automated decision-making technologies including profiling, where the processing of that data is not subject to a statutory or legal requirement.

## Roles and Responsibilities

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

The Governing Body of the School and the Headteacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the Data Protection Principles.

It is the responsibility of all staff to ensure that their working practices comply with the Data Protection Principles. Staff who do not comply with this policy may face disciplinary action.

The School have appointed a Data Protection Officer (DPO) who will have responsibility for all issues relating to the processing of personal data and will report directly to the Headteacher.

The Data Protection Officer will comply with responsibilities under the GDPR and will deal with Subject Access Requests, requests for rectification and erasure, data security breaches. Complaints about data processing will be dealt with in accordance with the Schools Complaints Policy.

## Data Security and Data Security Breach Management

- All staff are responsible for ensuring that personal data which they process is kept securely and is not disclosed to any unauthorised third parties.
- Access to personal data should only be given to those who need access for the purpose of their duties.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access.
- Data will be disposed of securely in accordance with the 'Information and Records Management Security' (IRMS) Retention Guidelines for Schools.
- The School will have in place a Data Breach security management process and serious breaches where there is a high risk to the rights of the individual will be reported to the Information Commissioner's Office (ICO) in compliance with GDPR.
- All staff will be aware of and follow the Data Breach security management process.

## Subject Access Requests

Requests for access to personal data or Subject Access Requests (SARs) will be processed by the Data Protection Officer. If staff receive a Subject Access Request they must immediately forward it to the DPO.

Subject Access Requests **must** be made in writing, either by letter or mail to the DPO.

The identity of the Requester **must** be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship with the child.

Subject Access should include:

- Name of Requester
- Correspondence address
- Contact number and email address
- Details of the information requested

When responding to requests we:

- May ask the Requester to provide 2 forms of identification.
- Will respond without delay and within the statutory 1 month of receipt of the request.
- Will provide the information free of charge.
- Where a request is complex or numerous, we will inform the Requester within 1 month of receipt that an extension to a maximum of two months may be necessary in order to respond to the request.

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 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.
- Contains personal data about other data subjects - in such instances we will take action to protect the data of the other subject by redacting it.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

Should we refuse a request, we will tell the Requester why, and tell them they have a right to complain to the ICO.

Records of all requests will be maintained.

Our DPO is Dr. B. Grundy and he can be contacted via Mrs. S. McLoughlin, School Business Manager.

## 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 (which includes most information about a pupil) within **15 school days** of receipt of a written request.

## Sharing data with third parties and data processing undertaken on behalf of the School

Personal data will only be shared with appropriate authorities and third parties where it is fair and lawful to do so. Any sharing will be undertaken by trained personnel using secure methods. Where third party undertakes data processing on behalf of the School e.g. by providing cloud based systems or shredding services, the School will ensure that there is a written agreement between the Data Controller and Data Processor (3<sup>rd</sup> Party) requiring the data to be processed in accordance with the Data Protection Principles and in accordance with the DPA.

## Ensuring Compliance

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing development, where changes to legislation, guidance or the School's processes make it necessary.

The School advises everyone whose personal data is held of the purposes for which it is processed and who it will be shared with. This is referred to as a "Privacy Notice" and is available on the School website.

The School will ensure Privacy Notices contain the following information:

- Contact information for the Data Controller and Data Protection Officer.
- Purpose of processing and legal basis.
- Retention period.

- Broad Principles of who we may share data with.
- Right to require rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

## CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individual's permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining CCTV is in use.

## Photographs, Additional Personal Data and Consents

Where the School seeks consents for processing personal data it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

## Links with existing policies and guidance

This Policy has been drawn up within the context of:

- Privacy Notice (pupil)
- Privacy Notice (staff)
- Data retention policy & schedule
- IT Policy including Acceptable use policy
- Data breach policy
- and other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

## Point of Contact

The first point of contact for all queries is the School Business Manager, Mrs. S. McLoughlin.

***Policy approved by Governing Body of Longmoor Community Primary School on 23<sup>rd</sup> May 2018***