

# Data Protection Policy

Midhurst CofE Primary School is committed to Safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. Our intention is that children will be safe, secure and happy, and enjoy their time as pupils at this school.

APPROVED (DATE)	NEXT REVIEW DATE
February 2024	February 2026

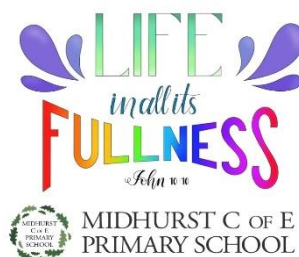
Approved by the Headteacher

Date: 28<sup>th</sup> February 2024

Signed:



HEADTEACHER



## **Vision**

At Midhurst CE Primary School we believe passionately in living life in all its fullness by developing the spiritual and holistic potential of each child. Our distinctively Christian values of kindness, peace, friendship, respect, creativity and forgiveness underpin the education and care we provide for the whole child, their family and school community.

## **Aims**

Our aim is that every child will reach their full potential by:

- learning to read so that they can read to learn.
- having the skills to write with purpose and fluency.
- becoming problem solvers through logic, reason and numeracy.
- knowing how to learn, what sort of learner they are and how they learn best.
- accessing a wide ranging, creative curriculum that is challenging and inspiring and caters for the needs of all.
- gaining knowledge, skills and understanding appropriate to a fast-changing world, so they can be self-reliant, adaptable and lead fulfilling and meaningful lives.
- being valued as an individual, who can share their concerns and can grow in confidence knowing their place in their class, their school, their local, national and international communities, wanting to help others and make a positive difference.
- being aware and able to make healthy choices physically and mentally. They will choose to keep active and develop positive attitudes to life and wellbeing.
- understanding that they are responsible for their own actions and take responsibility for them.

At Midhurst C of E Primary School, we strive to ensure that the whole school environment is a place that promotes learning, encourages challenge and independence and is as safe as possible. We believe that children should feel secure, happy, and valued as unique individuals so their educational, emotional, spiritual, and physical needs are met. We expect every child to make good progress and develop their wisdom, knowledge, skills and understanding of the world they live in.

We encourage enthusiasm and motivation across the school, enabling us all to be creative and imaginative in our work. The biblical teachings of Jesus underpin all we do, our priorities and decisions, collective worship, RE and across the curriculum. Our Christian values are alive and in action around the school. Our distinct Christian foundation supports children to cooperate, share and show respect for everyone, regardless of faith, culture or ethnic background and be responsible for their own behaviour.

## **Data Protection Policy**

Lead member of staff	Mark Jefferson
Governor approval delegated to Headteacher by FGB	Mark Jefferson
Date of publication	Feb 2024
Review date	Feb 2026

### **Introduction**

On the 25th May 2018 the General Data Protection Regulation (GDPR) became applicable and the Data Protection Act 1998 (DPA) was updated by the new Data Protection Act 2018 giving effect to its provisions.

This Policy sets out the manner in which personal data of staff, students and other individuals is processed fairly and lawfully.

The School collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the School. This 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 must therefore comply with the Data Protection Principles in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The School must be able to demonstrate compliance. Failure to comply with the Principles exposes the School and staff to civil and criminal claims and possible financial penalties.

The Schools registration number is Z7619530. This registration is renewed annually and up dated as and when necessary.

### **Aim**

This Policy will ensure:

The School processes person data fairly and lawfully and in compliance with the Data Protection Principles.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities under this policy.

That the data protection rights of those involved with the School community are safeguarded.

Confidence in the School's ability to process data fairly and securely.

### **Scope**

This Policy applies to:

Personal data of all School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the School.

The processing of personal data, both in manual form and on computer.

All staff and governors.

### **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 and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data 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 is processed.
6. Processed in a way 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 School will be able to demonstrate compliance with these principles.

The School will have in place a process for dealing with the exercise of the following rights by Governors, staff, students, parents and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including
- profiling.

### **Roles and Responsibilities**

The Governing Body of the School and the Head Teacher 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. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy

A designated member of staff, the Data Protection Officer, will have responsibility for all issues relating to the processing of personal data and will report directly to the Head Teacher.

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.

All staff will comply with the Schools Acceptable IT use Policy.

Staff who work from home must have particular regard to the need to ensure compliance with this Policy and the Acceptable IT use Policy.

Data will be destroyed securely in accordance with the 'Information and Records Management Society Retention Guidelines for Schools'.

New types of processing personal data including surveillance technology which are likely to result in a high risk to the rights and freedoms of the individual will not be implemented until a Privacy Impact Risk Assessment has been carried out.

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 the GDPR.

All staff will be aware of and follow the data breach security management process.

All staff will be aware of and comply with the list of Do's and Don'ts in relation to data security in Appendix A

### **Subject Access Requests**

Requests for access to personal data (Subject Access Requests)(SARs) will be processed by the Data Protection Officer. Generally, no fee is applicable. Records of all requests will be maintained.

The School will comply with the statutory time limits for effecting disclosure in response to a Subject Access Request. The statutory time period is one calendar month of receipt of the 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 a 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 requiring the data to be processed in accordance with the Data Protection Principles.

### **Ensuring compliance**

All new staff will be trained on the data protection requirements as part of their induction.

Training and guidance will be available to all staff.

All staff will read the Acceptable IT use Policy.

The School advises students whose personal data is held, 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 also provides a Privacy Notice to staff which is available on the School website.

The School will ensure Privacy Notices contains the following information:

- Contact Data Controller and Data Protection Officer
- Purpose of processing and legal basis. Retentions period. Who we share data with.
- Right to request rectification, erasure, to withdraw consent, to complain, or to know about any automated decision making and the right to data portability where applicable.

### **Photographs, Additional Personal Data and Consents**

Where the School seeks consents for processing person data such as photographs at events it will ensure that appropriate written consents are obtained. Those consent forms will provide details of how the consent can be withdrawn.

Where the personal data involves a child under 16 years written consent will be required from the adult with parental responsibility.

## Appendix A

### What staff should do:

- DO** get the permission of your manager to take any confidential information home.
- DO** transport information from school on secure computing devices (i.e. encrypted laptops and encrypted memory sticks). Wherever possible avoid taking paper documents out of the office.
- DO** use secure portable computing devices such as encrypted laptops and encrypted USB memory sticks when working remotely or from home.
- DO** ensure that any information on USB memory sticks is securely deleted off the device, or saved on a School shared drive.
- DO** ensure that all paper based information that is taken of premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
- DO** ensure that any confidential documents that are taken to your home are stored in a locked drawer.
- DO** ensure that paper based information and laptops are kept safe and close to hand when taken out off premises. Never leave them unattended. Particular care should be taken in public places (e.g. reading of documentation on public transport).
- DO** ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.
- DO** return the paper based information to the School as soon as possible and file or dispose of it securely.
- DO** report any loss of paper based information or portable computer devices to your line manager immediately.
- DO** ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information. When sending personal information by post the envelope should clearly state 'Private – Contents for Addressee only'.
- DO** ensure that when posting/emailing information that only the specific content required by the recipient is sent.
- DO** use pseudonyms and anonymise personal data where possible.
- DO** ensure that access to SIMS (or equivalent) is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

### What staff must not do:

- DO NOT** take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device. Any information must be taken to the destination directly and never left unattended during the journey.
- DO NOT** unnecessarily copy other parties into e-mail correspondence.
- DO NOT** e-mail documents to your own personal computer.
- DO NOT** store work related documents on your home computer.
- DO NOT** leave personal information unclaimed on any printer or fax machine.
- DO NOT** leave personal information on your desk over night, or if you are away from your desk in meetings.
- DO NOT** leave documentation in vehicles overnight.
- DO NOT** discuss case level issues at social events or in public places.
- DO NOT** put confidential documents in non-confidential recycling bins.
- DO NOT** print off reports with personal data (e.g. pupil data) unless absolutely

necessary.

**DO NOT** use unencrypted memory sticks or unencrypted laptops