Data Protection Policy

November 2026

Version 3.0

Date of approval by headteacher: 19.11.26

Date of ratification by governors:

Date of last review: 19.11.26

Date of next review: October 2029

1 Introduction

1.1 Sonning Common Primary School collects and uses personal data about staff, pupils, parents, carers and other individuals who come into contact with the school. This information is gathered to allow us to provide education and other associated functions. In addition, there is a legal requirement for us to collect and use personal data to ensure that our school complies with our statutory obligations.

1.2 Schools have a duty to be registered as Data Controllers with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website.

1.3 This policy is intended to ensure that personal data is processed in accordance with the

- *Privacy and Electronic Communications Regulations (PECR) 2003*
- *UK General Data Protection Regulation (UK GDPR) and Data Protection Act (DPA) 2018*
- *Data Use and Access Act 2025*

1.4 In practice, complying with these Acts means ensuring that any use of personal data is lawful, fair, transparent and secure, with appropriate safeguards and clear accountability in place. This applies to data regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

1.5 This policy should be read in conjunction with our Privacy Notices, which summarise the why we collect personal data, what we do with it, how long it is held and whether it is shared with any other organisation.

1.6 All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities and adhering to these guidelines.

2 Definitions

2.1 **Personal data** is information that relates to an identified or identifiable living individual. In a school this includes identity details, contact details, information about pupil behaviour and attendance, assessment results, staff recruitment information, staff contracts, staff development reviews, staff and pupil reference.

2.2 Data Protection legislation places obligations on all those who process personal data and defines the following roles:-

- ***Data Controller*** *– this is the School, as the School determines the purpose of processing i.e. decides how and why data is used.*
- ***Data Processors*** *– the person or organisation that processes data on behalf of the controller. The school is sometimes a data processor.*

- ***Data Subjects*** *– the individuals whose information is collected and processed (for example current and past pupils. parents, carers, members of staff, governors, volunteers, visitors)*
- ***ICO*** *– Information Commissioner's Office*

2.3 **Special category data** is personal data that's considered more sensitive and given greater protection in law. This includes

- *Racial or ethnic origin*
- *Political opinions*
- *Religious or philosophical beliefs*
- *Trade union membership*
- *Genetic information*
- *Biometric information (eg fingerprints)*
- *Health matters (eg medical information)*
- *Sexual matters or sexual orientation*

2.4 As a school we also consider this data to be sensitive information

- *Safeguarding information*
- *Pupils in receipt of pupil premium or free school meals (FSM)*
- *Pupils with special educational needs and disabilities (SEND)*
- *Children in need (CIN)*
- *Children looked after by a local authority (CLA)*

2.5 Schools process **criminal offence data** by storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means the school is processing criminal offence data. This applies even though the check has not revealed any conviction.

3 The Information Commissioner (ICO)

3.1 The Information Commissioner is the body that oversees compliance with Data Protection legislation and has powers to force organisations to process personal data lawfully.

3.2 The School, as a data controller, is registered with the ICO and maintains a record of the information it holds and the purposes for which it obtains and uses personal data (including disclosure in any form to third parties). These details must be kept up to date and are available for inspection by the Information Commissioner's Office.

3.3 Where a data subject is unhappy with some aspect of the processing of their personal information they have the right to complain to the Information Commissioner. The ICO recommend that any issues should be resolved locally between the School and the individual concerned where possible. Any enquiries subsequently received from the Information Commissioner will be referred to the School's Data Protection Officer.

4 Policy Statement

4.1 The Data Protection Act 2018 establishes seven enforceable principles which must be adhered to at all times. Sonning Common Primary School is committed to ensuring that all information is collected, processed, maintained and disclosed in accordance with these principles. Personal data will be:

- *processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')*
- *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')*
- *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*
- *accurate and where necessary, kept upto date; every reasonable step must be taken to ensure that the personal data that are inaccurate are erased or rectified without delay ('accuracy')*
- *kept in an form which permits identification of data subjects for no longer than necessary ('storage limitation')*
- *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organizational measures ('integrity and confidentiality').*
- *The data controller shall be responsible for, and be able to demonstrate compliance that, data is processed lawfully, fairly and in a transparent manner ('accountability')*

5 General Statement

5.1 The school is committed to maintaining these principles at all times, therefore the school will:

- *Inform individuals why the information is being collected when it is collected*
- *Inform individuals when their information is shared, and why and with whom it was shared*
- *Check the quality and the accuracy of the information it holds*
- *Ensure that information is not retained for longer than is necessary*
- *Ensure that when obsolete information is destroyed that it is done so appropriately and securely*
- *Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded*
- *Share information with others only when it is legally appropriate to do so*
- *Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests*
- *Ensure our staff are aware of and understand our policies and procedures*

6 Responsibilities

6.1 All employees, governors and any other individual handling personal information on behalf of the school have a responsibility to ensure that they comply with Data Protection legislation and the school's policies.

6.2 Governors and trustees check that the school:

- *monitors their data protection performance*
- *supports the data protection officer*
- *has good network security infrastructure to keep personal data protected*
- *has a business continuity plan in place that includes cyber security*

6.3 The school's data protection officer (DPO) is the headteacher, Rachel Salmons. As the school is an Oxfordshire maintained school queries will be sent to the OCC Data protection team dataprotectionofficer@oxfordshire.gov.uk

6.4 Senior leaders are accountable for:

- *deciding how the school uses technology and maintains its security*
- *deciding what data is shared and how*
- *setting school policies for the use of data and technology*
- *understanding what UK GDPR and the Data Protection Act covers and getting advice from the OCC data protection officer, as appropriate*
- *assuring governors that the school has the right policies and procedures in place*
- *making sure any contracts with third-party data processors cover the relevant areas of data protection*
- *making sure staff receive training on data protection every 2 years*

6.5 Staff training on data protection will include training on specific school processes such as:

- *personal data breach reporting processes*
- *the escalation of information rights requests*

6.6 All staff are made aware of what:

- *personal data is*
- *'processing' means*
- *their duties are in handling personal information*
- *the processes are for using personal information*
- *is permitted usage of that data*
- *the risks are if data gets into the wrong hands*
- *their responsibilities are when recognising and responding to a personal data breach*
- *the process is for recognising and escalating information rights requests*

6.7 There are extra requirements for any staff in school who collect, store or view personal data and they are responsible for:

- *making sure they have a legitimate need to process the data*
- *checking that any data they store is needed to carry out necessary tasks*
- *identifying any risks*
- *understanding the governance arrangements that oversee the management of risks*

6.8 Staff are responsible for making sure that pupils using personal data for projects or coursework do so appropriately. This includes being compliant when storing data.

7 Data subject rights

7.1 Data subjects have rights and control over the use of their personal data. These rights are:

- *the right to be informed*
- *the right of access*
- *the right to rectification*
- *the right to erasure*
- *the right to restrict processing*
- *the right to data portability*
- *the right to object*
- *rights in relation to automated decision-making and profiling*

8 Privacy Notices

8.1 Two privacy notices are in use, one for pupil data and one for staff data. The current privacy notices are available on the school's website. The privacy notices detail:

- *What personal data is being processed*
- *Why personal data is being processed*
- *On what lawful basis the personal data is being processed*
- *With whom the personal data is being shared and why*
- *How and for how long the personal data will be stored*
- *How a data subject can exercise their rights over their personal data*

- *Who to contact if there are questions or concerns about their personal data*
- *Our filtering and monitoring activities*

9 Data Breach Management Process

9.1 All breaches, or suspected breaches, of Data Protection legislation will be reported to the school's Data Protection Officer who will ensure the process is adhered to and ensure breaches are reported to the ICO where necessary. The process has 5 steps

9.2 **Detect and Verify**: we will identify any incidents (for example unauthorized logins, lost devices, data sent to the wrong recipient) and notify the DPO and IT support, legal and HR as soon as reasonably practical.

9.3 **Contain and Recover**: we will take immediate mitigating actions (for example isolating affected servers, revoking compromised access credentials) and preserve evidence (for example system logs) for analysis.

9.4 **Assess the Risk**: we will determine the likelihood and severity of the risk to individuals' rights and freedoms based on the type, volume and sensitivity of the data. We will classify the breach as near-miss, minor, standard reportable, or high risk.

9.5 **Notify the Authorities and Individuals**: we will report notifiable breachers to the ICO within 72 hours of becoming aware of it, detailing the nature of the breach, records affected and steps taken. We will directly inform affected individuals without undue delay if the breach poses a high risk to their rights.

9.6 **Evaluate and Learn**: we will record every personal data breach, even if not legally required to be reported externally, and then conduct a root cause analysis, patch security vulnerabilities, update policies and retrain staff to prevent reoccurances.

10 Subject Access Request Process

10.1 **How to submit**: You should make a request in writing (letter or email) to the headteacher via the school office (office@sonning-common.oxon.sch.uk). You can make a verbal request (over the phone or face-to-face) but we prefer a written request for record keeping.

10.2 **Proof of identity**: We may ask you to verify your identity (e.g., passport or driving licence) and confirm your parental responsibility if you are requesting records on behalf of a child.

10.3 **Cost**: Providing data is generally free of charge unless the request is manifestly unfounded, excessive, or repetitive.

10.4 **Response deadline**: We must respond within one calendar month of receiving the request (or from when identity verification is completed). This can be extended by up to two additional months for complex requests, if this is the case we will tell you in writing why we think this is a complex case. School holidays do not pause this deadline.

10.5 **What is included**: You can request general school records, attendance, reports, and correspondence. We will make every effort to search all records including emails, documents, spreadsheets, databases, record systems, CCTV, USB sticks and paper records. Note that we will redact third-party data (information about other children or staff) or exempt information before sending.

10.6 **Clarification**: We cannot ask the requester to narrow or reduce their request but we can ask for clarification of what specific information the requester is looking for. This might be helpful when the requester asks for a lot of information because they are not sure what they need. If you just want specific data we may be able to process the request more quickly than providing you with a full set of data.

10.7 If you already have access to the information you want to see, we can direct you to this. For example, you may already have access to personal data stored about your child in MCAS. In this case we do not have to treat this request as a SAR, provided you can access the information within one calendar month.

10.8 We can refuse to comply with a SAR if

- *a data protection exemption can be applied to all the personal information in scope of the request*
- *the request is manifestly unfounded or manifestly excessive*

Examples of exemptions that may apply to education settings include*:*

- *releasing the information would cause serious harm to a child*
- *releasing information would not be in the best interests of a child*
- *information relating to third parties*
- *legal advice sought and received from a lawyer*
- *information that may prejudice an investigation*

11 Complaints

11.1 Complaints will be dealt with in accordance with the school's complaints policy.

11.2 A data subject has the right to make a complaint at any time to the Information Commissioner Office, the UK the supervisory authority for data protection issues. The ICO's details are as follows:

The Information Commissioners Wycliffe House
Water Lane Wilmslow Cheshire SK9 5AF
website: www.ico.gov.uk

12 Dissemination

The Policy is available on the school web site and a paper copy is available on request from the school office.

13 Reviewing the Policy

This policy will be reviewed every 3 years by the Headteacher and monitored by the Governing Body to ensure that the Policy is relevant and up to date.

14 Appendix A Example Response to SAR

From:

To: [Name of Data Subject] **Date:** [Insert Date]

Subject: Response to your Subject Access Request (SAR)

Dear [Name of Data Subject],

Thank you for your data subject access request dated [Date of request], which we received on [Date of receipt]. You requested: *[Insert a brief, clear confirmation of what was asked for, e.g., "electronic copies of any personal data we hold about your child in our school records"]*.

We have conducted a reasonable and proportionate search of our records to locate the personal data we hold about you.

1. Your Personal Data

Please find enclosed/attached a copy of the personal data we process concerning you.

2. Mandatory Information (Article 15 UK GDPR)

In accordance with your rights under UK GDPR Article 15, we provide the following supplementary information regarding our processing of your data:

- **Purposes of processing:** [e.g., account management, service delivery, legal compliance]
- **Categories of personal data:** [e.g., name, contact details, transaction history, support logs]
- **Recipients or categories of recipient:** [e.g., internal staff, third-party cloud hosting providers, payment processors]
- **Retention period:** We plan to store your data for [insert retention period or criteria used to determine it].
- **Your rights:** You have the right to request rectification, erasure, or restriction of your data, and the right to object to processing. You also have the right to lodge a complaint with the Information Commissioner's Office (ICO).
- **Automated decision-making:** [State whether any automated decision-making or profiling takes place, including meaningful information about the logic involved].

3. Third-Party Data & Redactions

[Optional: In some instances, we have redacted or withheld certain information because it relates to another individual whose identity would be disclosed, or because an exemption applies under the Data Protection Act 2018 (Schedule 2)].

If you have any questions regarding this response, please contact us by email at office@sonning-common.oxon.sch.uk or by phone on 0118 972 2105.

Yours sincerely,

Mrs Rachel Salmons
Sonning Common Primary School Headteacher and Data Protection Officer

15 Appendix B SAR record example

Date SAR received	Received from	Brief description	Response sent (Who by & Date)	Brief summary (how it was responded to)