Shine as Lights in the World
Philippians 2.15

General Data Protection Regulation (UK GDPR) and Data Protection Policy

Version: 2.0 (March 2026)
Supersedes: March 2024 version
Next Review: March 2028 or earlier if legislation/guidance changes

Contents

1. Aims
2. Legislation and guidance
3. Definitions
4. The data controller
5. Roles and responsibilities
6. Data protection principles
7. Collecting and using personal data (lawful bases, fairness and transparency)
8. Sharing personal data (including international transfers)
9. Subject access requests and other individual rights
10. Parental access to the educational record
11. CCTV
12. Photographs and videos
13. Data protection by design and default (including children's safeguards)
14. Data security and storage of records
15. Disposal of records
16. Personal data breaches
17. Training
18. Complaints about our data protection handling
19. Monitoring and review
20. Links with other policies

Appendix 1: Personal data breach procedure
Appendix 2: Record of processing and retention summary (signpost)
Appendix 3: Key contacts

1. Aims

Our school aims to ensure that all personal data about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored, used and disposed of in line with applicable UK data protection and privacy law. This policy applies to all personal data, in any format (paper and electronic).

2. Legislation and guidance

This policy reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications Regulations (PECR).

It incorporates the amendments made by the Data (Use and Access) Act 2025 (DUAA). Most data protection provisions of the DUAA commenced on 5 February 2026, with a statutory complaints-handling requirement commencing on 19 June 2026. The school has implemented this ahead of time.

The policy is informed by guidance published by the Information Commissioner's Office (ICO), including the ICO's updated guidance on data protection by design and by default and subject access requests.

3. Definitions

Personal data: Any information relating to an identified or identifiable living individual (the 'data subject').

Special category data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data (for identification), health data, and data concerning a person's sex life or sexual orientation.

Criminal offences data: Personal data relating to criminal convictions and offences, or related security measures.

Processing: Any operation performed on personal data, whether automated or manual (e.g. collection, recording, organisation, storage, adaptation, retrieval, use, disclosure, erasure or destruction).

Data controller: The organisation which determines the purposes and means of processing personal data (the school).

Data processor: A person or body (other than an employee of the data controller) that processes personal data on behalf of the data controller.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Recognised legitimate interests (RLI): A statutory category of legitimate interests introduced by the DUAA. Where processing is necessary for certain recognised interests (e.g. safeguarding, emergency response, crime prevention, network and information security, and certain internal administrative purposes), no balancing test is required in addition to the necessity assessment.

Scientific research (statutory definition): The DUAA clarifies the scope of 'scientific research' in UK GDPR for applying research provisions, including certain commercial and non-commercial activities.

4. The data controller

Our school determines why and how personal data relating to pupils, parents and carers, staff, governors, visitors and others is collected and used, and therefore is a data controller under the data protection laws. The school is registered with and pays the required data protection fee to the Information Commissioner's Office (ICO), the UK's regulatory body for data protection.

5. Roles and responsibilities

Governing board – The governing board has overall responsibility for ensuring the school has appropriate governance in place to comply with data protection law, which includes strategic oversight of this policy and supporting procedures.

Data protection officer (DPO) – The DPO oversees and monitors this policy, advises on compliance, and is the first point of contact for individuals and for the ICO. The DPO reports annually to the governing board and advises it as needed.

The school's DPO is Julie Hemming, School Business Manager
Email: office.3257@wychwood-pri.oxon.sch.uk | Tel: 01993 830059

Headteacher – Acts as the representative of the data controller on a day-to-day basis and ensures appropriate resources and training are in place.

All staff – All staff must handle personal data in accordance with this policy and training; report concerns promptly; and seek advice from the DPO before new processing, capturing consent, drafting privacy notices, transferring data outside the UK or EEA where applicable, engaging new processors, or where a personal data breach is suspected.

6. Data protection principles

The school ensures that any processing of personal data that it does complies with the following UK GDPR principles.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

7. Collecting and using personal data (lawful bases, fairness and transparency)

We will only process personal data where a lawful basis applies and processing is necessary for that basis.

Lawful bases include: contract; legal obligation; vital interests; public task (exercise of official authority/public interest tasks); legitimate interests; consent; and recognised legitimate interests (RLI) introduced by the DUAA.

Where relying on RLI, we will ensure the processing is necessary for the recognised interest (e.g. safeguarding of children and individuals at risk, responding to emergencies, crime prevention and detection, network and information security, certain internal administrative transfers). No additional balancing test is required beyond the necessity assessment.

Special category and criminal offence data will only be processed where an appropriate condition in data protection law is met (in addition to a lawful basis).

We will provide clear privacy information when we collect personal data directly from individuals and will keep such information accessible via our website and on request.

We will only collect personal data that is adequate, relevant and limited to what is necessary; we will keep it accurate and up to date; and we will keep it no longer than necessary in line with our retention schedule.

8. Sharing personal data (including international transfers)

We will not share personal data with third parties without a lawful basis. Where we use data processors (e.g. IT suppliers), we put contracts in place with appropriate data protection clauses and conduct due diligence.

We share personal data with law enforcement and public bodies where required by law or where necessary for safeguarding or emergency response.

Where we transfer personal data outside the UK (or to a country without an adequacy regulation), we will implement appropriate safeguards such as International Data Transfer Agreements (IDTAs) or UK Addenda, and ensure supplementary measures where required.

9. Subject access requests and other rights of individuals

Individuals have the right to request access to their personal data (Subject Access Request, SAR) and to receive information on how it is processed.

Identity verification: the one-month response period starts when we have sufficient information to identify the requester; where necessary we will promptly request ID or clarification and the deadline will start/continue once received.

We will make reasonable and proportionate searches to locate information and will respond without undue delay and within one month unless an extension (up to two months in complex cases) is justified and communicated within the first month.

We may refuse or charge for manifestly unfounded or excessive requests, giving reasons and informing individuals of their right to complain to the ICO.

Children and SARs: Personal data about a child belongs to the child. Parents/carers may exercise rights on a child's behalf where the child is not competent to understand their rights; competency is considered on a case-by-case basis (children under 12 are generally unlikely to be competent).

Other rights include rectification, erasure, restriction, objection (including to public task/legitimate interests processing), portability (where applicable), and rights related to automated decision-making and profiling.

10. Parental access to the educational record

Parents or those with parental responsibility have a right of access to the pupil's educational record within 15 school days of a written request, free to view and with a reasonable fee for copies, subject to statutory exemptions.

11. CCTV

We use CCTV in designated areas to help keep the site safe and secure. We follow the ICO's code of practice and provide clear signage. Enquiries about CCTV should be directed to the School Business Manager.

12. Photographs and videos

We obtain written consent from parents/carers for the use of pupil images and recordings for school communications, marketing and promotional purposes, and we explain how they will be used.

Parents/carers may take images at school events for personal use (not generally subject to data protection law). We ask that images including other pupils are not shared on social media unless all relevant parents/carers have agreed, for safeguarding reasons and in line with the school's Use of Mobile Devices and Cameras in School policy.

When the school uses images, we avoid including additional personal information that would enable identification, wherever possible. Consent can be withdrawn at any time, after which we will cease further use and take reasonable steps to delete images we control.

13. Data protection by design and default (including children's safeguards)

We integrate data protection into processing activities and projects from the outset and throughout the lifecycle.

We conduct data protection impact assessments (DPIAs) where processing is likely to result in a high risk to individuals' rights and freedoms, or when introducing new technologies.

For online services likely to be accessed by children, we implement appropriate technical and organisational measures and age-appropriate safeguards (privacy by default).

We keep internal records of processing and ensure appropriate governance, training and regular review of controls.

14. Data security and storage of records

- Paper records and portable devices containing personal data are kept secure when not in use.
- Confidential papers are not left in accessible areas; where personal data must be taken off-site, it is signed out/in at the school office.
- Devices and accounts are protected with strong passwords; portable devices and removable media are encrypted.
- Staff using personal devices for school work must follow our Use of Mobile Devices and Cameras in School policy.
- When sharing data with third parties, we ensure appropriate security and contractual safeguards.

15. Disposal of records

Personal data that is no longer required, or is inaccurate and cannot be rectified, will be securely destroyed or deleted in line with our retention schedule. Certified third parties may be used for secure disposal where appropriate.

16. Personal data breaches

We take all reasonable steps to prevent personal data breaches. Suspected breaches must be reported immediately to the DPO and will be handled in accordance with Appendix 1.

Where required, we will notify the ICO within 72 hours of becoming aware of a notifiable breach and will inform affected individuals where there is a high risk to their rights and freedoms.

We note the ICO's strengthened investigatory and enforcement powers and will cooperate fully with investigations.

17. Training

All staff and governors receive data protection training at induction and periodic refreshers. Additional training is provided when legislation, guidance or school processes change.

18. Complaints about our data protection handling

The school maintains and follows a formal complaints procedure for concerns about how we handle personal information.

Individuals should raise concerns in writing to the DPO in the first instance. We will acknowledge complaints promptly and provide a written response setting out our investigation, decision and any actions taken.

If the complainant remains dissatisfied, they may escalate to the Headteacher and then the Chair of Governors. Individuals may also complain to the ICO at any time.

19. Monitoring and review

The DPO monitors compliance with this policy and supporting procedures. The governing board reviews this policy at least every two years or earlier if legislation or guidance changes.

20. Links with other policies

- Confidentiality
- Social media and Use of Mobile Devices policies
- Freedom of Information publication scheme
- Safeguarding and Child Protection policy
- Records Management and Retention schedule
- Complaints procedure

Appendix 1: Personal data breach procedure

1. Report immediately: Staff/processors must notify the DPO without delay of any suspected or actual personal data breach.
2. Containment and assessment: The DPO coordinates containment and investigates to determine whether personal data has been lost, disclosed, altered, destroyed or accessed unlawfully.
3. Risk evaluation: The DPO assesses likelihood and severity of risk to individuals' rights and freedoms.
4. Notification decisions: If the breach is likely to result in a risk to individuals' rights and freedoms, the ICO will be notified within 72 hours of awareness. Where the risk is high, affected individuals will be informed without undue delay, in clear language, describing the breach, likely consequences and measures taken.
5. Documentation: All breaches are documented (facts, effects, actions taken) whether or not notification is required.
6. Review and lessons learned: The DPO and Headteacher review incidents and implement improvements (training, process or technical controls).

Examples of school-related incidents include:

- Publication of a non-anonymised dataset on the school website (e.g. identifiable pupil results).
- Safeguarding records disclosed to an unauthorised recipient.
- Loss or theft of an unencrypted device containing personal data.
- Compromise of a third-party service provider leading to exposure of parent payment details.

Appendix 2: Record of processing and retention summary (signpost)

The school maintains an internal Record of Processing Activities (ROPA) and a retention schedule (e.g. based on the IRMS toolkit for schools). These documents list categories of data, purposes, lawful bases (including any RLI reliance), recipients, transfers, retention and security measures. Copies are available on request.

Appendix 3: Key contacts

Data Protection Officer (DPO): Julie Hemming, School Business Manager
Email: office.3257@wychwood-pri.oxon.sch.uk | Tel: 01993 830059

Supervisory authority: Information Commissioner's Office (ICO) – www.ico.org.uk

Approved by Governors: 19 March 2026