

Therefore, encourage one another and build each other up, just as in fact you are doing”

1 Thessalonians 5:11

Thatcham Park C.E. Primary & Nursery School,

Data Protection Policy



Our Christian values underpin our ethos; every child is valued and encouraged to achieve their full potential. Every member of our school community is encouraged to respect and value each other. We want our children to learn to understand and respect our common humanity, diversity and differences so that they can go on to form the effective, fulfilling relationships that are an essential part of life and learning.

Policy owner	Governing Board
Operational lead	Headteacher and School Business Manager
Data Protection Officer	Gerard Strong, SchoolDPO.com – gerard@schooldpo.com
School contact	Park Avenue, Thatcham, Berkshire RG18 4NP – 01635 870950
Document status	Approved by F&R September 2026
Review cycle	At least annually, and sooner following a material legal, regulatory or operational change

1. Purpose and scope

Thatcham Park C.E. Primary & Nursery School is committed to protecting personal data and respecting the privacy rights of pupils, parents and carers, staff, applicants, governors, volunteers, visitors, contractors and other members of the school community. This policy explains the principles and arrangements the school applies when it collects, uses, shares, stores and disposes of personal data.

This policy applies to all personal data processed by or on behalf of the school, in any format and wherever it is handled. It applies to governors, employees, agency staff, volunteers and contractors who process personal data for the school. It should be read alongside the school's privacy notices, retention schedule, information security arrangements, records of processing activities and related policies.

The policy sets the school's framework. Compliance also depends on the school following its procedures, maintaining accurate records and controls, training its people and reviewing practice.

2. Legal and regulatory framework

The school will process personal data in accordance with applicable data protection law, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018, as amended, including amendments made by the Data (Use and Access) Act 2025;
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 where relevant; and
- the Education (Pupil Information) (England) Regulations 2005 where they apply to access to, and transfer of, maintained-school pupil records.

The school also has regard to current guidance from the Information Commissioner's Office (ICO), the Department for Education (DfE) and relevant safeguarding bodies. Freedom of information and environmental information requests are governed by separate legislation and procedures, although a request may engage more than one regime.

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

3. Key terms

Personal data: information relating to an identified or identifiable living person.

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

Criminal offence data: personal data relating to criminal convictions and offences or related security measures.

Processing: any operation performed on personal data, including collecting, recording, organising, using, sharing, altering, storing, retrieving or deleting it.

Controller: the organisation that determines why and how personal data is processed. The school is the controller for most processing undertaken for its own purposes.

Processor: an organisation that processes personal data on the controller's instructions.

Data subject: the living person to whom personal data relates.

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

4. Data protection principles

The school is responsible for, and must be able to demonstrate, compliance with the UK GDPR principles. Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- processed securely, protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- supported by evidence of accountability, including appropriate policies, records, assessments, contracts, training and oversight.

5. Roles and responsibilities

5.1 Governing Board

The Governing Board has overall responsibility for ensuring that the school meets its legal obligations and manages information risk appropriately. It will receive appropriate assurance, approve this policy and ensure that sufficient resources and authority are available for data protection compliance.

5.2 Headteacher

The Headteacher is responsible for implementing this policy, establishing effective procedures and controls, ensuring that staff understand their responsibilities, escalating significant risks and ensuring that the DPO is involved appropriately and in a timely manner.

5.3 Data Protection Officer

The DPO is Gerard Strong of SchoolDPO.com (gerard@schooldpo.com). The DPO acts independently and reports to the highest management level on data protection matters. The DPO's tasks include informing and advising the school, monitoring compliance, advising on data protection impact assessments, supporting breach and rights-request handling, and acting as a contact point for data subjects and the ICO. The school will provide the DPO with access, information and resources necessary to perform these tasks and will avoid conflicts of interest.

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

5.4 School Business Manager and information owners

The School Business Manager coordinates local administration and record keeping. Leaders and system or information owners are responsible for ensuring that processing within their areas is documented, necessary, secure, accurate and supported by appropriate notices, retention rules and supplier arrangements. The allocation of operational tasks does not remove the controller's accountability.

5.5 All staff, governors and volunteers

Anyone handling personal data for the school must follow this policy, associated procedures and training; use only authorised systems; access only the information needed for their role; keep information secure; check before sharing; and report suspected breaches, rights requests, complaints and concerns immediately through the school's established route. Deliberate or negligent misuse may result in disciplinary or contractual action and, in some circumstances, personal legal liability.

6. What personal data the school uses

Depending on the individual and the purpose, the school may process identification and contact details; attendance and attainment information; special educational needs and disability information; safeguarding and welfare records; health and dietary information; behaviour and exclusion information; photographs, video and audio; communications; financial and funding information; admissions and transition information; employment, payroll and professional records; vetting information; access, device and system logs; and other information necessary to provide education, care and school administration.

The school may process special category data and criminal offence data where necessary and where an additional condition in data protection law is met. The school will maintain an appropriate policy document where required by the Data Protection Act 2018 and will apply enhanced safeguards to sensitive information.

7. Lawfulness, fairness and transparency

7.1 Lawful bases and conditions

Before processing personal data, the school will identify and document an appropriate lawful basis. These commonly include legal obligation, performance of a task in the public interest or exercise of official authority, contract, vital interests, consent and, where legally available and appropriate, legitimate interests. Public authorities cannot rely on legitimate interests for processing carried out in the performance of their public tasks.

Where special category or criminal offence data is processed, the school will also identify and document the relevant additional condition and any required safeguards. Information will not be used for a materially incompatible new purpose without assessing the legal position and, where required, providing further information to affected people.

7.2 Privacy information

The school will provide clear, accessible and age-appropriate privacy information at the point personal data is obtained or within the period required by law when it is obtained elsewhere. Privacy notices will explain, as applicable, the school's identity and contact details, the DPO, purposes and lawful bases, categories and sources, recipients, international transfers, retention, rights, complaint routes and any applicable automated decision-making. Notices will be reviewed when processing or legal requirements change.

7.3 Consent

The school will use consent only when it is freely given, specific, informed, unambiguous and genuinely optional. Consent requests will be separate and clear, recorded and as easy to withdraw as to give.

Where a child may give consent, the school will consider the child's competence and the specific legal context; it will not apply a blanket age rule. Withdrawing consent does not affect processing already

undertaken lawfully or processing supported

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

by another lawful basis.

8. Data quality and minimisation

The school will collect only information that is relevant and necessary for the stated purpose. Forms, systems and recurring data collections will be reviewed periodically. Reasonable steps will be taken to keep information accurate and current, particularly where inaccuracy could affect education, safeguarding, welfare, pay or other significant decisions. Staff and families should notify the school promptly when relevant details change.

Where an accuracy challenge arises, the school will consider the source and purpose of the record, distinguish fact from professional opinion where appropriate, record the challenge where the original entry must be preserved, and restrict use while accuracy is being verified when the law requires it.

9. Individual rights

Individuals may have rights to be informed, access their personal data, rectify inaccurate data, erase data, restrict processing, receive portable data, object to processing, and obtain safeguards in relation to solely automated decisions with legal or similarly significant effects. Rights are not absolute; which rights apply depends on the circumstances and lawful basis. The school will explain any lawful limitation or refusal and the right to complain.

Requests do not need to use legal terminology or a particular form. Any member of staff who receives a possible rights request must send it immediately to the Headteacher or School Business Manager and the DPO. The school will identify the request, verify identity or authority where reasonably necessary, keep an audit trail and respond without undue delay and within the applicable statutory period.

10. Subject access and education records

10.1 Subject access requests

A subject access request (SAR) may be made verbally or in writing and can be made to any part of the school. The school will normally respond within one month. It may pause the response period while awaiting reasonably required clarification about the information sought and may extend the period by up to two further months where a request is complex or numerous, provided the requester is told within the initial period and given reasons.

The school will conduct reasonable and proportionate searches. Responses will normally be provided free of charge and in the format required by law. Where permitted, a reasonable fee may be charged or a request may be refused if it is manifestly unfounded or excessive. Any decision to rely on an exemption, withhold third-party information, charge a fee or refuse a request must be documented and should involve the DPO.

10.2 Children, parents and carers

Personal data belongs to the child to whom it relates. A child who understands the request and its implications may exercise their own rights. A parent or carer may act with the child's authority or where it is otherwise appropriate and lawful, taking account of the child's competence, wishes, best interests and any safeguarding concerns. Parental responsibility does not create an automatic right to all of a child's personal data.

As a maintained school, Thatcham Park will also handle a parent's separate right to access their child's educational record under the Education (Pupil Information) (England) Regulations 2005. Where that regime applies, access must be provided within 15 school days of a written request, subject to the statutory restrictions and permitted fee. The school will identify whether a request is a SAR, an education-record request, or both, and apply the correct rules.

11. Sharing and disclosure

Personal data will be shared only where there is a clear purpose and lawful basis, the disclosure is necessary and proportionate, and appropriate security and accountability measures are in place. Routine

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

sharing will be reflected in privacy

information and, where appropriate, supported by a data-sharing agreement. The school will check identity, authority, accuracy, recipient, minimum necessary content and secure transfer arrangements before sharing.

The school may share information with bodies such as the local authority, Department for Education, health and social care services, safeguarding partners, emergency services, police, regulators, professional advisers, payroll or pension providers, examination bodies, receiving schools and approved suppliers where lawful and necessary. Data protection law does not prevent necessary and proportionate sharing to safeguard a child or another person. Staff must not delay an urgent safeguarding disclosure while seeking consent when consent is not the appropriate basis.

Disclosures about one person may contain information about others. The school will consider confidentiality, third-party rights, exemptions and redaction rather than applying a blanket rule. Significant or unusual disclosures will be documented and referred to the DPO where appropriate.

12. Suppliers, processors and contracts

Before appointing a supplier that will process personal data, the school will carry out proportionate due diligence covering security, privacy, resilience, data locations, subprocessors, deletion or return arrangements and relevant certifications or assurances. A compliant written contract must be in place before processing starts and must include the matters required by Article 28 UK GDPR.

The school will maintain oversight of processors, review material changes and incidents, and ensure that data is returned or securely deleted at the end of the service unless retention is legally required. A supplier may not determine new purposes for school data or appoint subprocessors except in accordance with the contract and law.

13. International transfers

Personal data will not be transferred outside the United Kingdom unless the transfer is lawful and documented. The school will establish where data and remote support access are located, whether UK adequacy regulations apply or an approved safeguard is required, whether a transfer risk assessment is needed, and whether supplementary technical or organisational measures are appropriate. Individuals will receive the information required by law about relevant transfers and safeguards.

14. Records of processing and accountability

The school will maintain records of processing activities (ROPA) that describe its purposes, categories of people and data, recipients, international transfers, retention and security measures. It will also maintain, as appropriate, data maps or asset registers, privacy notices, lawful-basis decisions, consent records, sharing agreements, processor contracts, data protection impact assessments, breach records, rights-request logs, complaint records, training records and retention arrangements.

Records will be kept sufficiently current to demonstrate how the school processes personal data in practice. Leaders and information owners must notify the operational lead and DPO before material new or changed processing is introduced.

15. Data protection by design and impact assessments

Data protection will be considered from the outset and throughout the life of projects, systems and processes. Default settings will limit collection, visibility, access and retention to what is necessary. The school will give particular weight to the interests and rights of children and will use age-appropriate design and explanations.

A data protection impact assessment (DPIA) must be completed before processing that is likely to result in a high risk to individuals, including certain uses of sensitive data, systematic monitoring, innovative technology, profiling or large-scale processing. The DPO will be consulted. The assessment will describe the processing, evaluate necessity and proportionality, identify risks and record measures to reduce them. If a high residual risk cannot be reduced, the school will consult the ICO before processing begins where required.

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

16. Information security

The school will use risk-appropriate technical and organisational measures to protect confidentiality, integrity, availability and resilience. Measures will include, as applicable:

- role-based access, prompt removal of leavers' access and periodic access reviews;
- strong authentication, secure password practices and multi-factor authentication where appropriate;
- approved devices, systems, storage and communication channels;
- encryption, secure configuration, patching, malware protection, filtering and monitoring;
- tested backup, recovery and business-continuity arrangements;
- physical security for paper records, devices and work areas;
- secure printing, transport and disposal, including confidential waste and certified destruction;
- careful checking of email recipients and attachments, with additional protection for sensitive transfers; and
- proportionate logging, monitoring, testing and supplier assurance.

Personal email, consumer cloud storage, unapproved messaging services and unapproved removable media must not be used for school personal data. When working remotely, staff must prevent overlooking or unauthorised access, secure devices and papers, and follow school procedures. Any loss, misdirection, unusual access or suspected compromise must be reported immediately.

17. Personal data breaches

All suspected or actual personal data breaches must be reported immediately using the school's incident route, even if the facts or impact are uncertain. Staff should take safe steps to contain the incident, preserve relevant evidence and avoid concealing or independently investigating it beyond their role.

The school will record all personal data breaches and promptly assess the data involved, affected people, likely consequences and containment. The DPO will be involved in assessment and advice. Where a breach is likely to result in a risk to people's rights and freedoms, the school will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware. Where it is likely to result in a high risk, affected individuals will also be informed without undue delay unless a lawful exception applies. The school will document the reasoning, response, lessons and follow-up action.

18. Retention, transfer and disposal

The school will retain personal data only for as long as it is needed for the purpose for which it was collected, including legal, safeguarding, accountability and records-management requirements.

Retention decisions will follow an approved retention schedule and any applicable statutory or sector requirements; the school will not apply a single blanket retention period to all records.

Records subject to a complaint, claim, investigation, safeguarding concern, audit or legal hold will not be destroyed until release is authorised. Pupil records will be transferred securely to receiving schools in accordance with education law and DfE requirements. When retention ends, personal data will be securely deleted, anonymised or destroyed, including copies held by processors where applicable.

19. Photographs, video, CCTV and monitoring

Photographs, video and audio will be used only for defined educational, safeguarding, security or communication purposes and in line with the relevant privacy information. The school will distinguish official school use from optional promotional use and will use consent only where consent is the appropriate lawful basis. Images will be stored, shared and retained securely, with particular care for safeguarding restrictions.

Any CCTV, access-control, device, network, filtering or monitoring activity must be necessary, proportionate, transparent and subject to appropriate access, retention and disclosure controls. Higher-risk monitoring will be assessed through a DPIA. Detailed arrangements should be set out in the relevant CCTV, online safety, filtering and monitoring, acceptable use or staff privacy documentation.

20. Artificial intelligence and automated decisions

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027

Staff must not enter personal, confidential

or sensitive school information into an artificial-intelligence service unless the service and proposed use have been formally approved. Proposed AI use must be assessed for lawful basis, transparency, accuracy, bias, security, supplier terms, data location, retention, intellectual property and the interests and rights of children. A DPIA will be completed where required.

Where the school uses solely automated processing to make a decision with legal or similarly significant effects, it will apply the safeguards required by law, including appropriate information, a route to make representations, meaningful human intervention and an opportunity to challenge the decision. Human users remain responsible for checking AI-assisted outputs and decisions.

21. Training and awareness

Governors, employees and other authorised users will receive appropriate data protection and information-security induction and refresher training. Additional role-specific training will be provided to those handling safeguarding information, special category data, rights requests, procurement, records management, breaches or high-risk systems. Completion and significant advice will be recorded, and learning from incidents and assurance work will be incorporated into future guidance.

22. Data protection complaints

The school will provide an accessible route for people to raise concerns about its handling of personal data. A complaint may be sent to the Headteacher, School Business Manager or DPO. Complaints will be logged, acknowledged within 30 days, investigated without undue delay, and answered with the outcome and any action. Where a final response cannot yet be given, the school will provide proportionate progress updates. Records of complaints and outcomes will be retained in accordance with the retention schedule.

Individuals may also complain to the Information Commissioner's Office. The school will normally ask them to raise the concern with the school first so that it has an opportunity to resolve it, but this does not remove their right to contact the ICO. ICO information is available at ico.org.uk/make-a-complaint/data-protection-complaints or by telephone on 0303 123 1113.

23. Assurance, monitoring and review

Compliance will be monitored through proportionate checks such as review of the ROPA and privacy notices, access reviews, training completion, supplier assurance, retention activity, incident and request trends, DPIAs and governance reporting. Findings will be assigned to an owner and tracked to completion according to risk.

The Governing Board will review this policy at least annually and sooner if there is a significant change in law, regulatory guidance, technology, school operations or risk. Approval of this policy does not replace the need to review and maintain the supporting procedures and records.

24. Related documents

This policy should be read with the current versions of the following, where applicable:

- privacy notices for pupils and families, workforce and other relevant groups;
- records of processing activities and information asset register;
- retention schedule and secure disposal procedure;
- subject access and individual rights procedure;
- personal data breach and incident-response procedure;
- data protection impact assessment procedure and template;
- information security, acceptable use, online safety and remote-working policies;
- safeguarding and child protection policy;
- CCTV, photography and recording arrangements;
- freedom of information policy and publication scheme;
- records of processor due diligence, contracts and data-sharing agreements; and
- artificial intelligence guidance or policy.

Status	Version	Date Approved	Review Date
Approved	2026	September 2026	October 2027