DATA PROTECTION POLICY

Park Road Academy Primary School | UK GDPR and Data Protection Act 2018

Document status	Ratified, November 2026
Policy owner	Senior Responsible Individual
Review cycle	Annual, or sooner following material legal or operational changes

Draft for trustee approval.

Document control and recent version history

Version	Date	Summary / approval
Draft 1	October 2026	Supplier due diligence, UK cloud residency, staff security and audit provisions
Draft 2	November 2026	SAR appendix, escalation route, version history and optional SAR form
Draft 3	November 2026	Data (Use and Access) Act 2025: recognised legitimate interests, automated decision-making and complaints procedure
Draft 4	November 2026	Updated SAR responsibilities, deadlines, searches and response requirements

Policy approval: Pending approval by the appropriate school governance body. Next review: to be set on approval.

1. Purpose and scope

Park Road Academy Primary School is committed to protecting personal information relating to pupils, parents and carers, staff, trustees, volunteers, visitors, contractors and others. This policy sets out the school's approach to lawful, fair, secure and accountable processing.

It applies to all staff, trustees and other individuals who process personal data on the school's behalf, in paper records, school systems, cloud platforms and communications.

2. Legal framework and principles

The school will comply with the UK GDPR, the Data Protection Act 2018 and relevant amendments, including applicable provisions of the Data (Use and Access) Act 2025.

Personal data must be processed lawfully, fairly and transparently; collected for specified purposes; limited to what is necessary; accurate; retained no longer than necessary; and protected by appropriate security. The school must be able to demonstrate compliance.

3. Roles and responsibilities

The school, as data controller where applicable, determines the purposes and means of processing. The headteacher and governing body or trustees provide appropriate oversight. The Senior Responsible Officer advises, monitors compliance and is consulted on new or materially changed processing.

All staff must handle personal information only for authorised purposes, follow school procedures, promptly report incidents and seek advice when unsure.

4. Lawful basis and sensitive information

Before commencing processing, the school will identify and document an appropriate Article 6 lawful basis. Where special category data is processed, an Article 9 condition and any relevant Data Protection Act 2018 Schedule 1 condition will also be documented. Criminal offence data is assessed separately under Article 10 and applicable domestic law.

Consent will only be relied upon where it is appropriate, freely given and capable of being withdrawn. Public task and legal obligation may be more appropriate for many statutory school functions.

5. Privacy notices and individual rights

The school will provide accessible privacy information explaining its purposes, lawful bases, recipients, retention arrangements, rights and relevant international transfers. Notices will be reviewed when new systems or purposes are introduced.

Staff must promptly forward requests to exercise data protection rights to the Senior Responsible Individual (SRI) at SRI@parkroadacademy.co.uk. Follow Appendix A for subject access requests. The Senior Responsible Officer (SRI) advises on statutory deadlines, exemptions and extensions where needed.

6. Supplier due diligence and approval — enhanced

Before any new supplier receives personal data, the school will carry out and record proportionate due diligence based on the nature, volume and sensitivity of the data and the risks to individuals.

Confirm the purpose of processing, each category of data requested and whether each field is necessary; challenge excessive or optional sensitive fields.

Identify whether the supplier acts as processor, independent controller or joint controller and document the arrangement.

Where the supplier acts as processor, obtain a written contract containing the mandatory UK GDPR Article 28 terms before processing starts.

Review technical and organisational security measures, including access restrictions, multifactor authentication, encryption, audit logging, breach response and secure upload methods.

Identify subprocessors, hosting locations, remote access arrangements, backups and any restricted international transfers and safeguards.

Confirm retention, secure deletion or return of data at contract end, and support for data subject rights.

Record the assessment, outstanding actions, residual risks, decision-maker and approval date. Do not upload live personal data until required controls are confirmed.

7. Cloud services, SharePoint and international transfers — enhanced

A supplier's statement that data is "held in the UK" will not, by itself, be treated as confirmation that all storage, support access, backup and other processing remain in the UK.

For cloud platforms, including Microsoft SharePoint, the school will seek appropriate assurance about tenant data residency, the location of relevant services and backups, authorised access from other countries, and subprocessors.

Any restricted transfer will be assessed under the UK GDPR international transfer rules, including adequacy regulations or appropriate safeguards where required. Findings will be recorded in the supplier assessment and ROPA.

8. ROPA, DPIA screening and privacy by design — enhanced

The school will maintain records of processing activities, including purposes, categories of individuals and data, recipients, transfers, retention and security measures, as applicable.

New suppliers, technologies, data-sharing arrangements and significant changes to existing processing must be referred for DPIA screening before implementation. A full DPIA will be completed where processing is likely to result in a high risk to individuals' rights and freedoms.

DPIAs will assess necessity, proportionality, risks and mitigating controls. Any high residual risk requiring prior consultation will be escalated appropriately before processing begins.

9. Staff security responsibilities — enhanced

Access personal information only where authorised and needed for work.

Use approved school systems and secure sharing methods; do not use personal accounts or unapproved storage.

Protect credentials, use multifactor authentication where provided, and never share passwords.

Verify recipients before sending information and apply appropriate encryption and access controls.

Do not download or retain personal data on local or personal devices unless specifically authorised and protected.

Keep paper records secure, use confidential disposal and promptly report suspected loss, disclosure or misuse.

Complete required data protection and information security training.

10. Data breaches

Staff must immediately report suspected or actual personal data breaches using the school's incident procedure. The school will record and assess incidents, contain risks, and determine whether notification to the ICO is required within the applicable statutory period (normally 72 hours after awareness for reportable breaches). Affected individuals will be notified where legally required.

11. Retention and secure disposal

Personal information will be retained only as long as necessary under the school's retention schedule and applicable legal obligations. Contracts with processors will specify arrangements for return or deletion at termination, including treatment of copies and backups.

12. Training, annual audit and review — enhanced

Relevant staff will receive data protection training at induction and regular refresher training. Completion and policy acknowledgements will be recorded.

The SRI will coordinate a proportionate annual review of the ROPA, supplier register, outstanding DPIA actions, access permissions, retention arrangements and material incidents. Findings and corrective actions will be documented and escalated as appropriate.

This policy will be reviewed annually and sooner if legislation, guidance, technology or school processing materially changes.

13. Related documents

See Appendix A for the Subject Access Request Procedure, Appendix B for the staff escalation route and Appendix C for the optional request form. This policy should also be read alongside the school's privacy notices, retention schedule, Data Breach Policy, Freedom of Information Policy and Publication Scheme, information security arrangements, CCTV policy, supplier due-diligence records, ROPA and DPIAs.

Approval record

14. Data (Use and Access) Act 2025 — legislative changes

The Data (Use and Access) Act 2025 amends the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications Regulations; it does not replace them. Relevant changes identified in the Department for Education's 2026 update took effect on 8 July 2026. The school will apply the provisions in force at the time of processing and review its procedures when further changes commence.

Recognised legitimate interests: The school will consider Article 6(1)(ea) and the specified recognised legitimate-interest purposes only where the statutory conditions apply. These may include certain safeguarding activities. This is distinct from ordinary legitimate interests and from public task. Staff must document the applicable purpose, necessity and any additional conditions; it is not a general permission to share pupil information.

Automated decision-making: Before implementing a system that makes solely automated decisions with legal or similarly significant effects, the school will assess whether the processing is permitted, identify any applicable restrictions involving special category data, and put in place the required safeguards. These include meaningful information, the ability to make representations, to contest a decision and to obtain human intervention where required. Any proposed use must be escalated for DPIA screening and appropriate approval.

Data protection complaints: Individuals may raise a complaint about how the school processes their personal information by contacting SRI@parkroadacademy.co.uk. Complaints will be logged, acknowledged within 30 days of receipt and investigated without undue delay. The school will explain its findings and any action taken, maintain records, and explain the right to complain to the Information Commissioner's Office. A complaint will be handled separately from, but coordinated with, any subject access request or other rights request.

Staff must promptly forward any data protection complaint to the designated lead and preserve relevant correspondence. The school will review complaint trends and use lessons learned to improve its controls.

Appendix A — Subject Access Request (SAR) Procedure

This appendix provides practical guidance for school staff. It supplements the school's data protection policy and should be read with current statutory requirements and ICO guidance.

A1. Recognising and escalating requests

• A SAR can be verbal or written, including by email, letter, telephone or another communication channel. The individual need not mention "SAR", "GDPR" or use a form.

• Staff who receive a request for someone's personal data from that person or their representative must forward it promptly to the SRI at SRI@parkroadacademy.co.uk. Record when the school received it and retain the original request or a note of what was asked verbally.

• The SRI coordinates the response, acknowledges the request promptly and records it and its deadline in the SAR register. The SRI advises on complex cases, exemptions and proposed refusals.

• The Headteacher will designate a deputy to monitor the SRI inbox and coordinate requests during absences and school closures. Staff should contact the Headteacher if the SRI is unavailable. School holidays count towards the SAR deadline.

• If staff suspect a breach or are uncertain about disclosure, they must escalate immediately rather than making their own disclosure decision.

A2. Identity, scope and timescales

• Verify the requester's identity and any representative's authority. If there are reasonable doubts about identity, ask promptly for proportionate evidence and use existing verification methods where suitable.

• Respond without undue delay and within one calendar month of receipt. Where identity evidence is reasonably required, the response period starts when the school receives sufficient evidence. If the deadline falls on a weekend or bank holiday, it moves to the next working day.

• Ask for clarification only where reasonably required to identify the requested information or processing. The requester may still ask for all their personal data. The clock pauses on the day clarification is requested and resumes the day after it is received. Record both dates, explain the effect on the deadline and provide any supplementary information that can reasonably be supplied without clarification within the original response period.

• The school may extend the deadline by up to two further months where necessary because of complexity or the number of requests from the same individual. Tell the requester within the initial month and explain the reasons for the extension.

• If the school refuses to act on a request, explain the reasons as far as the law permits and tell the requester about their right to complain to the ICO and seek a judicial remedy. Give this notice without undue delay and within the initial response period.

A3. Requests concerning children and third parties

• The right of access belongs to the child. Assess whether the child can exercise that right. A parent may act on behalf of a child who cannot exercise it independently, subject to the child's best interests, or with the authority of a child who can exercise it. Consider parental responsibility, any court orders, confidentiality and safeguarding risks before disclosure.

• Assess third-party information carefully and consider redaction or lawful exemptions. Do not assume that a parent is automatically entitled to all records about their child.

• Consult the SRI and safeguarding lead where records contain safeguarding allegations, family disputes or other sensitive third-party information.

A4. Park Road search checklist

Carry out reasonable and proportionate searches based on the scope of the request. Record which sources were searched and the reasons for any material limits. Consider the following sources where relevant.

• Arbor and other management / admissions records; Tapestry and nursery records; CPOMS safeguarding records;

• Microsoft 365 email, Teams, SharePoint and appropriate paper files;

• EntrySign, CCTV where applicable, wraparound and holiday club records;

• Information held by processors or service providers on the school's behalf, where within the scope of the request.

A5. Review, disclosure and record keeping

• Identify relevant personal data, review accuracy and exemptions, redact where appropriate, and arrange secure delivery to the verified recipient.

• Confirm whether the school processes the individual's personal data. Where it does, provide a copy of the personal data and the supplementary information required by UK GDPR Article 15, including the purposes, categories of data, recipients, retention period or criteria, applicable rights and the right to complain to the ICO. Include the available source of data collected elsewhere, applicable automated decision-making information and safeguards for relevant international transfers.

• Keep a SAR register recording receipt date, requester, identity/authority checks, scope, systems searched, key decisions, extension or pause reasons, disclosures and response date.

• Retain the request and response record according to the school's retention schedule.

Appendix B — Staff escalation route

Staff should contact the Senior Responsible Individual (SRI) at SRI@parkroadacademy.co.uk for advice or escalation on new systems, data sharing, lawful basis, consent, retention and international transfers. Follow Appendix A for SARs, the Data Breach Policy for suspected breaches and Section 14 for data protection complaints. Follow the school's safeguarding procedures for urgent safeguarding concerns.

The Headteacher should be informed through the school's internal escalation arrangements where appropriate. Staff and data subjects may contact the SRI directly without being required to escalate through the Headteacher first.

Appendix C — Optional Subject Access Request Form

This form is offered to make requests easier. It is not mandatory. A valid subject access request can be made without using this form.

Name of person whose information is requested

_____

Preferred contact email / telephone

_____

If acting for someone else: name, relationship and authority

_____

Information requested (records, dates, systems, if known)

_____

Preferred response method (email / post / other)

_____

Any accessibility requirements

_____

The school may request proportionate identity or authority evidence where necessary. Please send requests to SRI@parkroadacademy.co.uk or contact the school office.