Redbourn Park

# Data Protection Policy

**Safety | Empathy | Ambition**

| | |
|---|---|
| **Approved by** | **Richard McCabe, Proprietor/Chair** |
| **Policy owner** | **Data Protection Officer (Head of Operations)** |
| **Approval/effective date** | **August 2026; revised November 2026** |
| **Next review** | **August 2028** |
| **Applies to** | **Grovehill and Gaddesden; pupils aged 7-16; staff, contractors, volunteers and visitors** |
| **Version** | **2026/27** |

## Related policies

Complaints and Compliments Policy
Child Protection and Safeguarding Policy
Online Safety Policy
Staff Code of Conduct Policy
Staff Handbook

# Contents

1. Aims and scope....4
2. Legal framework....4
3. Definitions....4
4. Data controller and contact....5
5. Roles and responsibilities....5
5.1 Proprietor/Chair....5
5.2 Data Protection Officer....5
5.3 The Headteacher....5
5.4 Safeguarding information....5
5.5 Technical controls....5
5.6 Staff, contractors and volunteers....5
6. Principles and lawful bases....5
7. Collecting and using personal information....6
8. Sharing personal information....6
8.1 Safeguarding sharing....6
8.2 Processors and suppliers....6
8.3 International transfers....6
9. Individual rights and subject access....6
10. Children, parents and educational information....7
11. Biometric information....7
12. CCTV....7
13. Photographs and video....7
14. Artificial intelligence and automated decisions....8
15. Data protection by design and DPIAs....8
16. Information security and devices....8
17. Retention and disposal....8
18. Personal data breaches....9
19. Data protection complaints....9
20. Training and awareness....9
21. Monitoring and review....10
22. Related records and documents....10
Appendix 1 - Personal data breach record....11

## 1. Aims and scope

Redbourn Park is an independent specialist school supporting autistic pupils and pupils with complex needs. Protecting personal information supports the school's values of Safety, Empathy and Ambition: information is kept secure, its use is explained accessibly, each pupil's voice is respected, and only information needed to help pupils learn, thrive and remain safe is used.

This policy applies to personal information processed at Grovehill and Gaddesden, during off-site activities, through remote working, and on school-approved systems and devices. It applies to all pupils, parents and carers, staff, contractors, volunteers, visitors and other people whose information the school processes.

The school will:

- process personal information lawfully, fairly, transparently and securely;
- collect and use only what is necessary for a clear and documented purpose;
- keep information accurate, accessible only to authorised people and no longer than necessary;
- respect individual rights and provide accessible ways to exercise them; and
- respond promptly to concerns, requests, complaints and actual or suspected incidents.

## 2. Legal framework

This policy is informed by the UK General Data Protection Regulation (UK GDPR), as amended; the Data Protection Act 2018; the Data (Use and Access) Act 2025; the Privacy and Electronic Communications Regulations where applicable; and current Information Commissioner's Office and Department for Education guidance.

Redbourn Park Group Ltd is not treated as a public authority merely because it provides education. The public-task lawful basis will be used only where the particular activity has a clear basis in law. The school will identify the lawful basis that fits each processing purpose rather than applying one basis to all school activity.

Where another law requires or permits information to be processed, the school will record that legal basis and apply the data-protection principles alongside it.

## 3. Definitions

| Term | Meaning |
|---|---|
| **Personal information** | Information relating to an identified or identifiable living person. In this policy, personal data and personal information mean the same thing. |
| **Special-category information** | Information requiring additional protection, including health, race or ethnicity, religion or belief, political opinions, trade-union membership, genetics, biometrics used for identification, sex life or sexual orientation. |
| **Criminal-offence information** | Information about criminal allegations, proceedings, convictions or related security measures. |
| **Processing** | Any operation involving personal information, including collecting, recording, organising, using, sharing, storing, altering, retrieving, restricting, deleting or destroying it. |
| **Controller** | The organisation that decides why and how personal information is processed. |
| **Processor** | An organisation that processes personal information on the controller's behalf under written instructions. |
| **Data subject** | The person the personal information is about. |
| **Consent** | A freely given, specific, informed and unambiguous indication of agreement that can be withdrawn. |
| **Data Protection Officer (DPO)** | The independent adviser who monitors compliance, advises on obligations and acts as a contact for individuals and the ICO. |
| **Data Protection Impact Assessment (DPIA)** | A documented assessment used before processing likely to create a high risk to people's rights and freedoms. |
| **Biometric information** | Personal information produced by specific technical processing of physical, physiological or behavioural characteristics, such as fingerprints or facial templates. |

| Term | Meaning |
|---|---|
| **Personal data breach** | A security breach leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information. |
| **Solely automated significant decision** | A decision made without meaningful human involvement that produces legal or similarly significant effects for a person. |

# 4. Data controller and contact

Redbourn Park Group Ltd is the data controller for personal information processed through Redbourn Park Independent School at Grovehill and Gaddesden.

Joanna Carson is the Data Protection Officer. Questions, rights requests and data-protection complaints may be sent to joanna@redbournpark.co.uk or raised through the Headteacher or the school office. A concern about the DPO may be sent directly to Richard McCabe, Proprietor/Chair.

# 5. Roles and responsibilities

## 5.1 Proprietor/Chair

The proprietor/chair approves this policy, provides governance oversight and appropriate resources, receives independent reports from the DPO, considers significant risks and incidents, and provides final governance assurance.

## 5.2 Data Protection Officer

The DPO acts independently, advises on legal obligations, monitors compliance, supports DPIAs, oversees rights requests and data-protection complaints, advises on breaches, maintains compliance records, acts as the ICO contact and reports directly to the proprietor/chair.

## 5.3 The Headteacher

The Headteacher is responsible for local implementation at Grovehill and Gaddesden, prompt escalation of rights requests, complaints and incidents, local physical and access security, approved phone-storage arrangements, and operational oversight of Earwig and Google Classroom.

## 5.4 Safeguarding information

The designated safeguarding lead (DSL) is the safeguarding information-sharing lead and operational owner of CPOMS. A deputy designated safeguarding lead (DDSL) follows the agreed safeguarding route when the DSL is unavailable.

## 5.5 Technical controls

IT contractors implement and maintain authorised technical security, filtering and monitoring controls. The Headteacher holds operational responsibility, the DSL reviews safeguarding effectiveness and the proprietor/chair receives assurance. The school does not create an IT or ICT manager role through this policy.

## 5.6 Staff, contractors and volunteers

Everyone working for or on behalf of the school must follow this policy, use approved systems, protect credentials and devices, collect only what is needed, complete required training, and report requests, complaints and actual or suspected incidents immediately.

# 6. Principles and lawful bases

The school applies the seven data-protection principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

Before processing starts, the school will select, document and communicate the lawful basis appropriate to each purpose. The seven available bases are consent, contract, legal obligation, vital interests, public task, recognised legitimate interests and legitimate interests.

Special-category information requires both an Article 6 lawful basis and an Article 9 condition. Where the Data Protection Act 2018 requires it, the DPO will identify the relevant Schedule 1 condition and establish an

Appropriate Policy Document. Criminal-offence information requires an Article 6 basis and official authority or another applicable legal condition.

The DPO will establish and maintain a record of processing activities and ensure that the lawful bases, purposes, retention and recipients are reflected in appropriate privacy information.

## 7. Collecting and using personal information

The school may process information needed for admissions, education, EHCP delivery and review, safeguarding, health and wellbeing, attendance, behaviour support, communication, staffing, finance, legal duties, site security and service improvement. The precise information and lawful basis will depend on the purpose.

Information may be obtained from the person, their parent or carer, previous settings, local authorities, health and social-care partners, staff observations, approved systems, CCTV or other lawful sources. People will be given appropriate privacy information unless a legal exception applies.

Privacy information will be concise, clear and accessible. Depending on individual need, the school may use Easy Read wording, visual prompts, symbols, signing, AAC, verbal explanation, additional processing time, a trusted adult or an advocate. A communication difference will not prevent a pupil from expressing a preference, making a request or raising a concern.

Staff must take reasonable steps to keep information accurate and up to date. Significant corrections must be recorded and, where appropriate, shared with recipients of the inaccurate information.

## 8. Sharing personal information

Before sharing personal information, the school will identify a lawful purpose, share only what is necessary and proportionate, confirm the recipient, use an appropriately secure method and record significant decisions.

### 8.1 Safeguarding sharing

Consent is not normally required where information sharing is necessary to safeguard a child. Concern about data protection must never delay proportionate action needed to protect a pupil.

The DSL will normally decide and record safeguarding disclosures, including what was shared, with whom, why and whether consent was obtained. In the DSL's absence, a DDSL will follow the safeguarding escalation route. In an emergency, staff must act to protect the child and record and escalate the decision as soon as possible.

### 8.2 Processors and suppliers

A processor must be subject to an appropriate written contract, security and due-diligence checks, documented instructions and arrangements for return or secure deletion. The DPO must be involved before a new processor handles sensitive or high-risk information.

### 8.3 International transfers

Personal information will not be transferred outside the UK unless the DPO has confirmed that a lawful transfer mechanism and any required risk assessment and supplementary safeguards are in place.

## 9. Individual rights and subject access

Depending on the circumstances and lawful basis, people may have rights to be informed; access their information; correct inaccurate information; have information erased; restrict processing; receive portable information; object; and receive safeguards for solely automated significant decisions.

A subject access request may be made verbally, in writing or through any accessible communication method. It does not need to mention data-protection law or use a particular form. Any staff member receiving a possible request must send it to the DPO immediately.

The school will respond without undue delay and normally within one month. Where legally permitted because a request is complex or several requests have been made, the period may be extended by up to two further months. The requester will be informed within the original month.

The school will make a reasonable and proportionate search. Where necessary and legally permitted, it may seek clarification to identify the information requested. Identity evidence will be requested only where there is reasonable doubt and will be proportionate to the risk.

Information will be clear, accessible and supplied securely. Responses are normally free. The school may charge a reasonable fee or refuse a request only where the law permits, including when the request is manifestly unfounded or excessive. Applicable exemptions and third-party rights will be considered and documented.

## 10. Children, parents and educational information

The personal information and associated rights belong to the pupil. Competence to exercise those rights will be assessed individually, considering the pupil's maturity, understanding, communication and the nature of the information. The school will not apply a fixed age threshold.

A parent or representative may act where the pupil authorises them or where it is otherwise lawful and appropriate. Before disclosure, the school will consider the pupil's rights, wishes, best interests and any safeguarding risk.

As an independent school in England, Redbourn Park does not apply the separate maintained-school parental entitlement to receive an educational record within 15 school days. Requests for a pupil's personal information will be considered under subject-access law and any other applicable legal duties.

## 11. Biometric information

The school does not currently operate an automated biometric-recognition system.

No biometric system may be introduced without proprietor approval, DPO advice, a DPIA, appropriate pupil and parental consultation, compliance with applicable law and a suitable non-biometric alternative.

## 12. CCTV

CCTV is used where necessary and proportionate to support site safety, security, safeguarding and the prevention or investigation of incidents. It will not routinely be used to monitor staff performance.

The Headteacher is the operational owner of CCTV at Grovehill and Gaddesden. The DPO oversees data-protection compliance and authorised IT contractors may provide technical support.

Recordings are held locally on circular recording equipment and are not made available through the public internet. Routine footage is normally retained for approximately three to four weeks and is then automatically overwritten on a rolling basis.

Relevant footage may be isolated and retained for longer where necessary for a safeguarding matter, incident, complaint, insurance matter, law-enforcement request or legal claim. It will be kept only for as long as needed for that purpose.

Access is restricted to specifically authorised people and recorded where appropriate. Signs and privacy information will identify CCTV use and purpose. Cameras will not be installed in areas with a heightened expectation of privacy without exceptional justification and a DPIA.

The system does not use facial recognition or other biometric identification. Audio must remain disabled unless it is separately assessed, approved and communicated. Requests for footage showing an individual will be handled as subject access requests while protecting the rights of others.

## 13. Photographs and video

A photograph or video is personal information where a person is identifiable from the image or its context, even if their name is not included.

The school will distinguish educational, administrative, safeguarding and promotional uses and identify the appropriate lawful basis for each. Where pupil choice can appropriately be offered, information and options will be accessible and any decision will be recorded.

Where consent is used, withdrawal affects future use. The school will take reasonable steps to remove an image from channels it controls where required, but cannot guarantee recall of printed material or copies already lawfully obtained by others.

Staff must use school-approved equipment and storage. Personal phones or personal cloud accounts must not be used to take or store pupil images unless expressly authorised for an exceptional purpose with appropriate safeguards.

## 14. Artificial intelligence and automated decisions

TeachMate AI is approved only for planning and basic tasks using generic or genuinely anonymised information. Staff must not enter pupil, family, staff or other personal information; special-category or criminal-offence information; confidential case details; or information from CPOMS, Earwig or Google Classroom.

TeachMate outputs must be checked by a competent member of staff. They must not be relied upon as the sole basis for safeguarding, educational, employment or other decisions affecting an individual.

No other AI service may process school information without prior DPO approval, supplier and processor checks, assessment of international transfers and a DPIA where required.

Entering personal information into an unauthorised AI service is an actual or suspected security and data-protection incident. It must be reported immediately and assessed under section 18.

The school does not make decisions producing legal or similarly significant effects solely through automated processing. Any proposed introduction requires proprietor approval, a DPIA, transparent information, meaningful human review and a route to challenge the decision.

## 15. Data protection by design and DPIAs

Privacy and security must be considered before new systems, suppliers, monitoring, data sharing or material changes begin. The DPO must be consulted early enough to influence the design.

A DPIA will be completed where processing is likely to create a high risk, including certain new technologies, systematic monitoring, large-scale or sensitive processing, or processing involving vulnerable children.

An unresolved high risk must be escalated to the proprietor/chair and, where legally required, the ICO before processing begins. Approved controls and actions from a DPIA must be implemented and reviewed.

## 16. Information security and devices

The school will apply proportionate organisational and technical safeguards, including:

- individual accounts, role-based least-privilege access and prompt removal of leaver access;
- multi-factor authentication for staff cloud, remote-access and privileged accounts where supported;
- secure credential management, screen locking, encryption, patching, logging and tested backups;
- approved secure transfer methods and appropriate controls for removable media;
- secure paper storage, clear-desk and clear-screen practice and confidential disposal;
- technical filtering and monitoring operated by IT contractors through the approved responsibility structure; and
- regular review of access to CPOMS, Earwig, Google Classroom and other systems holding personal information.

Personal devices must not store or process school personal information unless approved under a documented arrangement providing appropriate encryption, MFA, access separation and remote revocation or wiping.

Personal phones will be stored and managed under the arrangements set by the Headteacher. They must not be used for pupil photography or school personal information unless expressly authorised for an exceptional purpose.

## 17. Retention and disposal

The DPO will establish and maintain a controlled retention schedule covering the school's main records. Periods will be based on legal requirements, safeguarding needs, limitation periods and documented operational necessity. Personal information will not be retained indefinitely or under an unjustified blanket period.

Until the controlled schedule is approved, the DPO will document and approve retention decisions for significant record categories, including safeguarding and CPOMS, EHCP and health information, staff records, CCTV, images, system logs, complaints and breach records.

Paper and electronic records will be securely destroyed or anonymised when no longer required. Disposal through a contractor must be covered by appropriate contractual and destruction-assurance arrangements.

## 18. Personal data breaches

Staff and contractors must immediately report an actual or suspected breach to the DPO and the Headteacher. They should take safe containment action but must not conceal the incident or destroy evidence.

Safeguarding implications must be reported immediately to the DSL. Technical incidents must also be escalated to the IT contractors. If the DPO is unavailable or involved in the incident, the matter must be escalated directly to the proprietor/chair.

The DPO will:

- start and maintain an incident record and establish when the school became aware;
- contain and investigate the incident and preserve relevant evidence;
- assess risks to affected people, including additional vulnerability or safeguarding risk;
- notify the ICO without undue delay and, where feasible, within 72 hours where the breach is not unlikely to create a risk to people's rights and freedoms;
- inform affected people without undue delay where the risk is high;
- document the reasons for any decision not to notify; and
- record corrective actions, owners, deadlines and lessons learned.

Reporting an incident in good faith will not itself lead to disciplinary action. Any separate concern about deliberate, reckless or repeated misconduct will be considered fairly under the appropriate employment process.

## 19. Data protection complaints

General handling will follow the school's Complaints and Compliments Policy. This section supplements that policy with requirements applying specifically to data-protection complaints. If timescales conflict, the legal requirements in this section take precedence.

A data-protection complaint may be made verbally, in writing, through an accessible communication method, by emailing the DPO at the address in section 4, or through the Headteacher or the school office. Any staff member receiving a complaint must forward it to the DPO immediately. A complaint concerning the DPO will be sent to the proprietor/chair.

The school will:

- acknowledge the complaint within 30 days;
- begin appropriate enquiries without undue delay and investigate fairly, accurately and proportionately;
- keep the complainant updated without undue delay, including explaining material delays;
- record the complaint, acknowledgement, evidence, communications, outcome and resulting actions; and
- provide a clear outcome, any corrective action and information about the right to raise the concern with the ICO.

The complainant may request reasonable adjustments, an alternative format, communication support, a trusted adult or an advocate. Making a complaint will not adversely affect the person's access to education, support or services.

## 20. Training and awareness

Staff will complete appropriate data-protection and security training at induction before access is provided, with annual refreshers and additional role-based training for the DPO, DSL/DDSLs, the Headteacher and people handling rights requests or sensitive records.

Contractors and volunteers will receive information and training proportionate to their access. Completion will be recorded. Targeted refreshers will follow significant legal or operational change, an incident, a complaint or identified non-compliance.

## 21. Monitoring and review

The DPO will monitor implementation and report significant findings, risks, complaints and breaches to the proprietor/chair. Monitoring may include audits of access, records, contracts, privacy information, DPIAs, requests, complaints, incidents, retention and disposal.

This policy will be reviewed by August 2028 and at least every two years thereafter. It will be reviewed sooner following material legal or operational change, a serious incident, new high-risk processing or significant ICO or Department for Education guidance.

## 22. Related records and documents

This policy should be read with the Complaints and Compliments Policy, Child Protection and Safeguarding Policy, Online Safety Policy, Staff Code of Conduct Policy and Staff Handbook.

The DPO will establish, maintain or commission the following controlled records where applicable:

- pupil/parent, workforce, website and CCTV privacy information;
- the record of processing activities and Appropriate Policy Document where required;
- the retention schedule and secure-disposal evidence;
- processor contracts, supplier checks, DPIAs and international-transfer records;
- subject access, data-protection complaint and personal-data-breach registers;
- CCTV signage, access, retention and assessment records; and
- the TeachMate AI approval and control record.

# Appendix 1 - Personal data breach record

The DPO may adapt the format to the circumstances, but every incident record must contain enough information to demonstrate the assessment and actions taken.

| Record field | Information to record |
|---|---|
| **Report details** | Reporter, site, date, time and immediate contact details. |
| **Incident timing** | Incident date/time, discovery date/time and when the school became aware. |
| **What happened** | Clear description of the incident, affected systems, devices, paper records or suppliers. |
| **Information affected** | Categories, sensitivity, approximate volume and whether special-category or criminal-offence information is involved. |
| **People affected** | Number and categories of people, including children or people with additional vulnerability. |
| **Likely consequences** | Potential physical, emotional, safeguarding, financial, reputational or other harm. |
| **Containment and recovery** | Immediate action, evidence preserved, recovery steps and responsible people. |
| **Escalation** | DPO, Headteacher, safeguarding and technical notifications, with times. |
| **Risk assessment** | Likelihood, severity, vulnerability and overall conclusion. |
| **ICO decision** | Whether notification is required, reasons, deadline, submission time and reference. |
| **Affected-person decision** | Whether people must be informed, reasons, communication and support provided. |
| **Corrective action** | Actions, owners, deadlines, completion evidence and lessons learned. |
| **Sign-off** | DPO review and governance assurance by the proprietor/chair where appropriate. |