Privacy Notice for Parents/Carers and Pupils

This privacy notice explains how and why the School collects, uses, stores and shares personal information about pupils and their parents, carers and family members (e.g. siblings or grandparents). It should be read with the School's Data Protection Policy, Retention and Deletion Policy, CCTV Policy, Photography and Social Media Policy, AI Policy and any more specific notice provided for a particular service.

The School is the Data Controller for the personal data described in this notice. This means that the School decides why and how personal data is used.

The School's Data Protection Officer (DPO) oversees and monitors our data protection compliance. You can contact the DPO via email dpo@robertclack.co.uk

This notice reflects the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (DUAA).

What Personal Data we hold

We only collect information that is relevant to our functions. Depending on the pupil and the services required, this may include:-

- ◊ Identity and Contact details: name, previous names, date of birth, sex, address, emergency contact details, unique pupil number, admission number and identifiers;
- ◊ Characteristics (ethnicity, first language, nationality, country of birth, religion, court orders, identification documents, pupil premium and free school meal eligibility, looked-after status);
- ◊ Admissions, previous school attendance records (e.g. sessions attended, number of absences and absence reasons, punctuality, exclusions and alternative provision);
- ◊ Curriculum, subjects studied, assessments, attainment, progress, predicted grades, examination entries and results, qualifications, coursework, teacher observations, educational records and transition information;
- ◊ Careers education, advice and guidance, intended destinations, post-16 applications, work experience and participation in education, employment or training;
- ◊ Examination access arrangements, candidate identifiers, examination scripts, coursework declarations, malpractice investigations and information shared with awarding organisations;
- ◊ Behaviour, sanctions, suspensions, permanent exclusions, managed moves and alternative provision;
- ◊ Relevant medical information (e.g. health conditions, medication, allergies, GP details, dietary needs, accidents, first aid, immunisation and school nursing information);
- ◊ Biometric information where used for services such as cashless catering or access control;
- ◊ Special educational needs and disabilities (SEND), education health and care plans, support plans, access arrangements and professional reports;
- ◊ Safeguarding, child-protection, early-help, pastoral, welfare and behaviour information, including referrals and professional involvement;
- ◊ Photographs, video and audio recordings, CCTV images;
- ◊ Clubs, trips, transport, music-tuition, meal and payment information;

- ◊ Online account details, device identifiers, IP addresses, audit logs, internet filtering and monitoring alerts, and use of school systems;
- ◊ Correspondence, complaints, requests, consent or preference records; and
- ◊ Information needed to protect pupils and staff, manage emergencies, investigate incidents and meet legal duties.

We may also receive and hold information from other organisations, including previous schools, local authorities, social services and the Department for Education.

Special Category and Criminal Offence Data

Some personal information needs additional protection. This includes:

- ◊ Racial or ethnic origin
- ◊ Religious or philosophical beliefs
- ◊ Health information (physical or mental)
- ◊ Sexual orientation or sex life
- ◊ Genetic or biometric data used for identification
- ◊ Political opinions or trade union membership

The School uses special category information only where permitted by data protection law. This may include when:

- ◊ we have your explicit consent
- ◊ it is necessary to protect someone's vital interests
- ◊ it is required for reasons of substantial public interest, as set out in data protection law

Safeguarding records may also contain criminal offence or allegation information. This information will only be processed where authorised by law and with appropriate safeguards.

For more information, please see our Data Protection Policy.

Where the information comes from

The School collects information directly from pupils, parents and carers and through day-to-day school activity. We may also receive information from:

- ◊ Previous, current or future schools, nurseries and education providers;
- ◊ The local authority, Department for Education (DfE), other government bodies and commissioned services;
- ◊ Health bodies, school nurses, immunisation and screening teams, GPs and other clinicians;
- ◊ Children's social care, early-help services, virtual schools, police, courts and safeguarding partners;
- ◊ SEND professionals, educational psychologists, therapists and support services;
- ◊ Approved education, IT, assessment, safeguarding and administration suppliers; and
- ◊ Publicly available sources where this is necessary and lawful.

Why we collect and use Personal Data

We use pupil and family data to:

- ◊ admit pupils, provide education, support learning and monitor attainment and progress;
- ◊ identify and meet SEND, health, accessibility, pastoral and welfare needs;
- ◊ safeguard children, prevent harm, respond to emergencies and manage behaviour and attendance;
- ◊ manage transition from primary school, movement between secondary schools and progression into sixth form, further education, apprenticeships, employment or other post-16 provision;
- ◊ manage curriculum choices, examinations, qualifications, careers education, work experience and post-16 progression;
- ◊ provide information to awarding organisations, careers services and post-16 education or training providers where necessary and lawful;
- ◊ communicate with families and manage school meals, clubs, trips, music and other services;
- ◊ take and use photographs or recordings for teaching, safeguarding, identification, school communications and, where appropriate, publicity;
- ◊ operate secure IT, filtering, monitoring, visitor-management, CCTV and other safety systems;
- ◊ meet statutory reporting, census, assessment, attendance, public-health and funding requirements;
- ◊ manage complaints, legal claims, audits, inspections, research, planning and service improvement; and
- ◊ keep accurate records and administer the School effectively.

We do not use your data for automated decision-making or profiling. If this changes, we will update this privacy notice and inform you.

Lawful Basis for Processing

The lawful basis depends on why the information is used. The School mainly relies upon:

- ◊ Article 6(1)(c) - legal obligation, where education, safeguarding, attendance, health and safety, equality, census or other law requires the processing;
- ◊ Article 6(1)(e) - public task, where processing is necessary for the School's official functions and duties in the public interest;
- ◊ Article 6(1)(d) - vital interests, where necessary to protect someone's life;
- ◊ Article 6(1)(b) - contract, in limited cases where processing is needed for a contract with the individual; and
- ◊ Article 6(1)(a) - consent, where a genuine choice can be offered, for example some optional publicity uses.

The School does not normally rely on consent for core education, safeguarding or statutory functions because consent can be withdrawn. Where we do rely on consent, it can be withdrawn at any time without affecting processing already carried out.

Photographs, video, audio and social media

The School may take photographs, video or audio for pupil identification, safeguarding, assessment, displays, learning records, performances, school publications and communication with families. Access is limited according to the purpose.

Identifiable images used on public-facing channels - such as the School website, prospectus, newsletters available to the public, Facebook, Instagram, X or other approved social-media accounts, will be managed under the School's Photography and Social Media Policy. The School will use public task as the lawful basis where the use is necessary for an official school communication and the law permits it. Families will be told how to express a preference or object. A refusal will not affect a pupil's education. In any other circumstances the school will seek consent.

The School takes additional care where publication could place a child at risk. The School will not normally identify a child by full name alongside a public image and will not publish images of looked-after children or pupils with relevant safeguarding restrictions unless specifically assessed and authorised.

Parents and visitors may be asked not to photograph or record certain events, or not to post images of other children online. Images captured by families for their own personal or household use are generally outside data protection law, but the School may impose event rules to protect children.

Where the School uses biometric information, for example for cashless catering, it will obtain the written consent required by the Protection of Freedoms Act 2012. Alternative arrangements will be provided where consent is not given. If a pupil objects to or refuses the use of their biometric information, the School will not collect or use it, even where parental consent has been provided.

Artificial Intelligence (AI)

The School may use approved AI-enabled tools to support teaching, learning, accessibility, assessment and administration. This may include drafting or summarising non-sensitive content, generating teaching resources, supporting feedback, or identifying patterns for staff review.

- ◊ Staff remain responsible for decisions and must check AI output for accuracy, bias and suitability.
- ◊ Only the minimum personal data necessary may be used. Information will be anonymised or pseudonymised where practicable.
- ◊ Staff and pupils must not enter personal, special category or confidential information into public or unapproved generative-AI tools.
- ◊ An AI supplier must be approved, contractually controlled and security-assessed before personal data is used.
- ◊ The School will not use AI to make a solely automated decision that has a legal or similarly significant effect on a pupil or family without a lawful basis, suitable safeguards, meaningful information, human intervention and a route to challenge the decision.
- ◊ A data protection impact assessment (DPIA) will be completed where the proposed use is likely to result in a high risk to pupils or other individuals.
- ◊ AI-generated or AI-assisted information will not be accepted without appropriate staff review where it may affect assessment, predicted grades, behaviour, safeguarding, examination arrangements, careers advice or other significant decisions about a pupil.

A particular AI tool may have its own supplementary privacy information. AI use is also governed by the School's AI and Information Security policies.

Smart glasses, wearable cameras and personal recording devices

Smart glasses and other wearable devices can capture images, audio, video, location and nearby people's personal information without this being obvious. Pupils, parents, visitors and staff must not use a recording function on school premises or at a school activity unless the School has expressly authorised it for a defined purpose or approved it as a reasonable adjustment.

Where authorised, the School will specify what may be recorded, who may access it, where it is stored and when it is deleted. Suspected unauthorised recording may be managed under relevant school policies and treated as a safeguarding, behaviour, employment or data-security matter.

Who we share information with

The School only shares information needed for the relevant purpose. The School does not need consent where another lawful basis permits or requires sharing. Recipients may include:

- ◊ the local authority and its commissioned providers, including admissions, attendance, SEND, safeguarding, public-health, virtual-school and education-support services
- ◊ the DfE, including statutory school census, assessment and daily attendance collections, and bodies acting on its behalf;
- ◊ schools, nurseries, alternative provision and other settings a pupil attends or transfers to;
- ◊ NHS bodies, school nursing, immunisation and screening services, emergency services and health professionals;
- ◊ children's social care, safeguarding partners, early-help services, police, courts and tribunals;
- ◊ Ofsted, auditors, professional advisers, insurers, awarding organisations, examination bodies, careers services providers and government agencies;
- ◊ colleges, sixth forms, apprenticeship providers, training providers and employers providing work-experience placements, where relevant and lawful;
- ◊ catering, transport, clubs, trips, music, photography and payment providers where relevant;
- ◊ approved IT, MIS, cloud, communications, safeguarding, assessment and learning-platform providers acting under contract; and
- ◊ research and survey organisations where lawful, with data anonymised or minimised where possible.
- ◊ Suppliers and service providers (e.g. IT platforms, HR)
- ◊ Central and local government
- ◊ Professional advisers and consultants
- ◊ Charities and voluntary organisations
- ◊ Professional bodies

We do not share information about pupils with anyone unless the law and our policies allow us to do so.

The School uses carefully selected third-party providers to host, store or process information and to deliver School services. This may include providers of management information systems, cloud and IT services, learning and assessment platforms, safeguarding and monitoring systems, communications,

payments, catering, visitor management, health services, clubs and trips. Providers acting on the School's behalf may only use the information necessary for the agreed purpose, must follow the School's written instructions and are required by contract to keep it secure.

Some organisations, such as the local authority, Department for Education, NHS or another school, act as independent data controllers and are responsible for their own use of the information.

Youth support services – pupils aged 13 and over

Once a pupil reaches the age of 13, the School may provide information to the local authority or its provider of youth support services. These organisations have responsibilities relating to the education and training of young people aged 13 to 19 under section 507B of the Education Act 1996. This enables them to provide youth-support services and careers advice.

Before the pupil reaches the age of 16, a parent or carer may request that no information other than the pupil's name, address and date of birth is shared for this purpose. Once the pupil reaches the age of 16, this right passes to the pupil.

Information may also be shared where necessary with post-16 education and training providers to support the pupil's progression. Further information about local youth-support and careers services is available from the Local Authority

Department for Education and the National Pupil Database

The School is legally required to provide information through statutory collections, including the school census and assessment collections. The DfE may link information from schools, local authorities and awarding bodies in the National Pupil Database (NPD), use it for education functions, research and statistics, and share it where permitted by law.

The School also shares daily attendance data with the DfE in accordance with the School Attendance (Pupil Registration) (England) Regulations 2024. This may be transferred securely from the School's management information system using Wonde.

DfE National Pupil Database privacy notice

DfE guidance on daily attendance data

International Transfers

Some approved suppliers may process or support information from outside the UK. Before a restricted transfer takes place, the School will ensure there is a lawful transfer mechanism and appropriate protection, such as UK adequacy regulations, the UK International Data Transfer Agreement, the UK Addendum to standard contractual clauses, and any required transfer risk assessment. Supplier details may be obtained from the School or DPO.

Security

The School uses organisational and technical measures designed to protect information against accidental loss, unauthorised access, alteration or disclosure. These include access controls, staff training, multi-factor authentication where appropriate, encryption, secure transfer methods,

backups, supplier contracts and incident-management procedures. Access is limited to people who need the information for their role.

How long we keep information?

Information is retained in accordance with the School's Retention and Deletion Policy, legal requirements and operational need. Core pupil and safeguarding records may need to be kept for long periods and transferred securely to a pupil's next school. Other records, such as unsuccessful admissions information, routine correspondence, CCTV and system logs, are kept for shorter periods. When information is no longer required, it is securely deleted or destroyed. A copy of the retention schedule is available from the School.

Your Rights

Depending on the lawful basis and circumstances, a pupil or other individual has the right to:

- ◊ be informed about how personal data is used;
- ◊ ask for access to personal data and receive a copy (a subject access request);
- ◊ ask for inaccurate data to be corrected and incomplete data completed;
- ◊ ask for erasure or restriction in certain circumstances;
- ◊ object to processing in certain circumstances, including where public task is relied upon;
- ◊ receive certain information in a portable format where the right applies;
- ◊ withdraw consent at any time where consent is the lawful basis; and
- ◊ obtain human intervention, make representations and challenge a qualifying significant automated decision.

These rights are not absolute. For example, the School may need to retain information to meet a legal obligation, protect a child, establish a legal claim, or protect another person's rights.

A pupil may exercise their own rights where they have sufficient understanding. A parent or person with parental responsibility may make a request on a pupil's behalf where it is appropriate and, in the pupil’s best interests. The School may need evidence of identity, parental responsibility or authority.

There is no fixed age at which a pupil becomes able to exercise their own data protection rights. As a general guide, a child aged 12 or over may be capable of making their own subject access request, but this will depend on their maturity, understanding and the nature and sensitivity of the information requested. Each case will be considered individually. Where a pupil has sufficient understanding, the School will normally seek their authority before responding to a request made on their behalf.

Requests should be sent to the School or its DPO using the contact details below. Please explain what you are asking about and provide dates, names or other details that will help us locate the information.

Under the DUAA, the School will make reasonable and proportionate searches when responding to a subject access request and may pause the response period while awaiting reasonably required information.
A request does not need to quote legislation or follow a legal, template or AI-generated format. You may use any support you need to make a request. To help us understand and locate what you actually want, please explain the request in your own words and, where possible, identify the subject matter, approximate dates, relevant members of staff and type of record or communication.

The right of access is a right to personal data, not an automatic right to copies of every document or email in which a person's name or email address appears. A request for 'all emails' will therefore be assessed to identify which emails contain the requester's personal data. Information about other people may be redacted or withheld where the law requires.

If a request is unclear, or the School holds a large amount of information, we may ask for clarification that is reasonably required to identify the personal data being requested and provide an effective response. The response period may be paused while we await that clarification. If clarification is not provided, the School will interpret the request as reasonably as possible using the information available and carry out reasonable and proportionate searches.

Access to the education record

In addition to data protection rights, a parent of a pupil at a maintained school may request access to, or a copy of, the pupil's educational record under the Education (Pupil Information) (England) Regulations 2005. The School normally responds within 15 school days. Limited copying charges and statutory exemptions may apply. This is separate from a pupil's right of access under the UK GDPR.

How the School uses cookies

The School website and online services may use cookies or similar storage and access technologies for essential functions, preferences, security and analytics. Where consent is required, users will be offered a choice.

Cookies are small files placed on your device that help improve website functionality and user experience. We use cookies to:

- Analyse website traffic
- Improve site navigation and usability

You can set your browser to refuse cookies or alert you when cookies are being sent. For more information, visit:

- http://www.aboutcookies.org
- http://www.allaboutcookies.org

Contact

If you have any queries or would like to discuss anything about how your personal information is handled, please contact our Data Protection Officer: dpo@robertclack.co.uk

Complaints

If you complain about how the School uses personal data, we will acknowledge the complaint within 30 days and investigate it without undue delay. We will tell you the outcome and explain how you can take the matter further. You may also complain to the Information Commissioner's Office (ICO), although the ICO will usually expect you to raise the matter with the School first.

Alternatively, you can make a complaint to the Information Commissioner:

Report a concern online

casework@ico.org.uk

0303 123 1113

Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

We review this notice regularly and when our use of personal data changes. The current version will be published on the School website and made available from the School office. Where a change is significant, we may also notify families directly.