

Garrett Hall Primary School Data Protection Policy (GDPR)



February 2026

Policy adopted: 23rd March 2026

Policy to be reviewed: March 2027

Signed on behalf of Governing Body : _____

Signed by the Headteacher : _____

Document history

School:	Garrett Hall Primary School
Date adopted by Governing Body:	
Signed (Chair):	<i>S. Chappell</i>
Signed (Headteacher):	<i>T.A. Beaty</i>

Date reviewed:	Comments:

Garrett Hall Primary School is committed to ensuring that the privacy of all our stakeholders is fundamental to our everyday practice, and that, as a school, we remain fully compliant with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

This document outlines what personal information we hold about the children who attend our school, why we hold this information, and who we share it with. It also explains your rights as a parent/carer in relation to accessing this information and the process to follow should you wish to do so.

Your Rights Under UK GDPR

In addition to the rights already outlined, individuals have the right to request erasure of personal data, the right to restrict processing, the right to object to processing carried out under public task or legitimate interests, the right to data portability where processing is based on consent or contract and carried out by automated means, and the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects. Where processing relies on consent, that consent may be withdrawn at any time. To exercise any of these rights, please contact the Data Protection Officer (DPO).

Data Breaches

A personal data breach is any incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. We maintain procedures to detect, report and investigate such incidents. Where a breach is likely to result in a risk to individuals' rights and freedoms, we will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within 72 hours of becoming aware of it. Where a breach is likely to result in a high risk to an individual, we will also inform the affected person(s) without undue delay. All breaches are logged and reviewed to prevent recurrence.

Lawful Bases for Processing Personal Data

Processing Special Category Data

We process special category data about pupils, parents/carers, staff and volunteers, including health information, ethnicity, religion or belief, biometric and safeguarding information, and data relating to special educational needs. Under Article 9 UK GDPR, this data is processed under one or more of the following conditions: substantial public interest (including safeguarding of children and individuals at risk), provision of health or social care, obligations in employment and social protection law, and explicit consent where appropriate. Additional safeguards, including access controls and need-to-know restrictions, are applied to this information.

Garrett Hall Primary School processes personal data under the lawful bases set out in Article 6 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Most information we collect and use is processed because it is necessary for the school to carry out its official functions as a public authority (public task) and to comply with our legal obligations (legal obligation) under education, safeguarding and health and safety legislation. In limited circumstances we rely on consent (for example, certain uses of pupil images or specific online platforms); consent is optional and can be withdrawn at any time without detriment. Where processing is required to protect someone's life, we rely on vital interests. Where applicable to staff and volunteers, some processing may be necessary for a contract or legitimate interests, balanced against individuals' rights.

What personal information do we collect? Who provides this information? Where do we store it?

ARBOR

When a pupil joins Garrett Hall, we request the following information from the child's parent/carer. If the child transfers from another school, this information will also be provided to us by the previous school.

We collect the following information:

- Child's Name
- Child's UPN Number
- Child's Date of Birth
- Child's Home Address
- Child's Ethnicity
- Child's Gender
- Child's Religion
- Child's Medical Practice
- Allergy or medical information regarding the pupil
- Free School Meal or Pupil Premium Information
- Information about previous schools and home addresses (if applicable)



- Names of any siblings
- Parent/Carer's Name
- Parent/Carer's Home Address
- Parent/Carer's E-mail Address
- Name and contact number of any identified emergency contacts
- Child's attendance
- Child's End of Early Years, Phonics, Multiplication, KS1 & KS2 data

This information is stored on Arbor, a secure web-based management information system. The School Office Administrator is responsible for managing this system, including inputting, transferring, and updating the information stored within it.

Only authorised members of staff can access data on Arbor. Some basic information (child's name, date of birth, address and emergency contact details) is also accessible to staff through secure pupil information folders stored in the school office.

Paper copies of annual parent/carer contact forms are also retained securely.

Information we may share without parental consent

How Long We Keep Personal Data

We retain personal data in line with statutory requirements and the Information and Records Management Society (IRMS) Records Management Toolkit for Schools. Different categories of information are kept for different periods based on legal, regulatory and operational needs. For example, the pupil educational record is retained until a pupil reaches the age of 25; child protection records are retained for 25 years; CCTV footage is retained for one month; and routine administrative records for shorter periods. At the end of the relevant retention period, data is securely destroyed or deleted in accordance with our disposal procedures. A detailed retention schedule is available on request from the school office.

There are circumstances in which the school must share a child's personal information without the initial consent of the parent/carer. These include sharing with:

- Social Services – to support their legal responsibility to safeguard children
- The Local Authority – to enable them to carry out their statutory duties relating to education and welfare
- The Department for Education – to meet statutory data collection requirements
- Government services such as:
 - Police – for legal investigations and child protection purposes
 - NHS – for emergency medical treatment
- Your child's new school when they transfer (sent via a secure Department for Education system)

The school also permits Arbor to integrate with other secure systems such as CPOMS, ParentPay, Sonar (Juniper), Parent Bookings, and similar platforms. These systems may receive necessary personal data such as a pupil's name, date of birth, and contact details.

Use of Third-Party Data Processors

International Transfers of Personal Data

Where personal data is transferred or accessed outside the United Kingdom, we ensure appropriate safeguards are in place. Depending on the destination and service, these may include the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses, or transfers to

countries covered by a UK adequacy decision. Further details of specific safeguards for each service provider are available on request.

We engage third-party service providers (processors) to deliver certain functions, including our management information system, safeguarding and assessment platforms, communications and payments systems, and educational apps. Each processor acts only on our documented instructions and is bound by a written Data Processing Agreement that meets Article 28 UK GDPR requirements. These contracts require appropriate technical and organisational measures, prohibit unauthorised sharing, and include audit and deletion provisions to protect personal information.

Additionally, the school may share information with professional support agencies such as Speech & Language Services, ATSA, School Counsellors, Family Support Workers, SEN Teams, Educational Psychologists, etc. Permission is always sought first unless safeguarding laws require otherwise.

CPOMS

We also collect and store the following information on CPOMS, our secure safeguarding and pastoral management system:

- Behaviour incidents
- Welfare concerns regarding a pupil
- Minutes from meetings between staff and pupils or parents/carers
- Information relating to legal orders, court agreements, or court proceedings



Most information is entered by school staff, although information may also be provided by parents/carers, visitors, other parents/carers, community members, or professionals such as police or social workers.

Due to the sensitivity of safeguarding data, only Senior Leaders and members of the Safeguarding Team have full access to all pupil records on CPOMS.

Other staff only see information relevant to the pupils they teach. All staff have individual secure login credentials.

SHARED DRIVES (School Network and OneDrive)

Teachers have access to a school-based shared drive and a cloud-based shared drive (OneDrive), both accessible in school and remotely.

Most stored files consist of teaching resources and planning materials containing minimal personal data.

However, some folders contain detailed personal information, including:

- Individual Pupil School Reports
- In-year (Interim) and End-of-Year (Summer) reports
 - Academic performance, attitudes to learning, behaviour, school values, and attendance

Reports are kept while the pupil remains at Garrett Hall and for up to three years after they leave, after which they are deleted.

SEND Folders

- ✓ Documents for pupils on the SEN register, including individual needs and support plans
- ✓ Reports from external agencies (Educational Psychologists, School Nurse, etc.)
- ✓ Information is regularly shared with parents/guardians and a child's new school if they transfer

Photograph Folder

- ✓ Photos taken throughout the year to document learning

- ✓ Parents/carers provide written permission annually
- ✓ Photos remain on the shared drive while the pupil attends the school and for one year after leaving, then deleted
- ✓ Photos stored temporarily on iPads but not transferred are deleted at the end of the academic year

Assessment Folders

- ✓ Data on attainment and progress
- ✓ National Data Scores
- ✓ Shared with parents/carers and the pupil's next school when transferring

SONAR

Teachers and senior staff use Sonar Tracker by Juniper Education, a cloud-based assessment platform that:

- Tracks pupil progress through formative and summative assessment data
- Identifies learning gaps
- Supports targeted intervention
- Enables leaders to generate reports and monitor pupil outcomes



PARENTPAY

Garrett Hall uses ParentPay as a secure online payment system for:

- School meals
- Trips
- Events and activities



It also functions as the school's main communication system for sending letters, reminders, newsletters, and notifications. ParentPay uses parent/carer contact details imported securely from Arbor.

PARENT BOOKINGS

Parent Bookings is used to organise:

- Parents' evening appointments
- Performance and event bookings
- Meeting schedules



Parents/carers book available timeslots online.

SEESAW

Consent for Online Services

Some online services used in school require consent for children under 13. In such cases, the school obtains parental consent in accordance with Article 8 UK GDPR and UK law. We explain clearly the purpose of the service and the data involved, and we record consent decisions. Consent is voluntary and can be withdrawn at any time. Pupils are not permitted to sign up independently to online services that process personal data without the appropriate permissions in place.



Seesaw is used by Early Years, Key Stage 1, and The Ark for:

- Sharing messages, photographs, and work samples with families
- Creating digital portfolios of children's learning
- Facilitating communication between school and home

Parents/guardians receive secure individual login details.

Paper-based information stored in school

The Headteacher holds whole-school assessment folders with data on every pupil and notes from pupil progress meetings.

The front office retains individual class files containing:

- Child's name and address
- Medical details
- Parent/carer names and contact details

The school also stores SEND and Child Protection Folders for individual children

- These are kept for 25 years
- Information is only shared with Government Agencies/Services when formally requested

Information shared to enable access to apps and websites

To enable pupils to access educational apps and online learning platforms, the school may share:

- Child's name
- Date of birth
- Year group

This information is used to generate a secure login and password.

None of the systems we use are allowed to share any information with third parties, advertisers, or marketers.

Use of Facebook and the School Website

The school uses Facebook to communicate and share significant events or celebrations.

This may include:

- Photographs of children
- Information about pupil achievements

Content remains online unless the school removes it or the account is deleted.

The school website is also used for communication and publicity.

Photographs are only used with parental permission.

CCTV

The school uses CCTV cameras around the site.

- Recordings are kept for one month before deletion
- Only Senior Leaders, the Pastoral Leader, and the Office Administrator can view the footage
- The CCTV company also has access due to live links to their external office
- Footage is used to manage and investigate incidents
- Police may request footage for investigations — parental consent is not required for this

Your Rights

Parents/carers have the right to:

- Request access to personal data held about you or your child
- Request corrections to inaccurate data
- Be informed if the school cannot comply and receive a written explanation
- Contact the Information Commissioner's Office (ICO) if you are dissatisfied

For concerns, please contact:

Mr Graves – Designated Data Protection Officer Email: dpo@garretthallprimary.example.org

Tel: 01942 883340

ICO: <https://ico.org.uk/>