Privacy Notice for Pupils & Parents of Cobham Montessori School

Contents

1. Introduction 1
2. The personal data we hold 1
3. Why we use this data 2
4. Our lawful basis for using this data 4
5. Collecting this data 5
6. How we store this data 5
7. Who we share data with 6
8. Your rights 8
9. Complaints 9
10. Contact us 9

---

1. Introduction

Under UK data protection law, including the **UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025**, individuals have a right to be informed about how our school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils at our school**.

This privacy notice applies while we believe your child is not capable of understanding and exercising their own data protection rights.

If you consider that your child is able to understand their rights over their own personal data (generally considered to be age 12, you should instead request our privacy notice for pupils to see what rights they have over their own personal data.

We, Cobham Montessori School, The Hall, 21-23 Spencer Road, Cobham, Surrey KT11 2AF Tel. 01932 863397 are the 'data controller' for the purposes of UK data protection law.

2. The personal data we hold

We hold personal data about pupils at our school to support teaching and learning, to provide pastoral care and to assess how the school is performing.

Personal data that we may collect, use, store and share (when appropriate) about you or your child includes, but is not restricted to:

- Contact details, contact preferences (such as your name, address, email address and telephone numbers), dates of birth, identification documents
- Records of learning progress
- Pupil and curricular records
- Financial Information related to payment of fees, bank details, bursaries and EYFE grant funding;
- Behaviour Records and Exclusion information
- Attendance information
- Details of any safeguarding information including court orders or professional involvement
- Details of families' circumstances
- Details of any support received, including care packages, plans and support providers
- Information about your child's use of our information and communications systems, equipment and facilities (e.g. school computers)
- Records of your correspondence and contact with us
- Details of any complaints you have made
- Records of filtering and monitoring of online activity (including use of school IT systems, devices, and networks)
- Records relating to requests for social transition (including parental consent, risk assessments, and decisions made)
- Biological sex information (which must be recorded accurately wherever sex is recorded)

We may also collect, use, store and share (when appropriate) information about you or your child that falls into 'special categories' of more sensitive personal data. This includes, but is not restricted to:

- Information about any medical conditions we need to be aware of, including physical and mental health
- Photographs and video images captured in school
- Information about characteristics, such as ethnic background or special educational needs (SEN)
- Information about incidents of child-on-child sexual harassment, sexual violence, or harmful sexual behaviour
- Information about incidents involving the making or sharing of nudes or semi-nudes (including AI-generated or altered images)

We may also hold data that we have received from other organisations, including other schools, professional advisers and local authorities.

3. Why we use this data

We collect and use the data listed above to:

a) Support pupil learning

b) Monitor and report on pupil attainment and progress

c) Provide appropriate pastoral care

d) Protect pupil welfare

e) Assess the quality of our services

f) Administer admissions waiting lists

g) Administer school property and operations

h) Comply with our legal and statutory obligations, including the law regarding data sharing

i) Make sure our information and communication systems, equipment and facilities (e.g. school computers) are used appropriately, legally and safely

j) Keep you informed about the running of the school (such as emergency closures) and events

k) Process payments for school services

We will only use your or your child's personal information for the purposes for which we have collected it, unless we reasonably consider that we need to use it for any other reason and that reason is incompatible with the original purpose. If we need to use your or your child's personal information for an unrelated purpose, we will notify you and explain the legal basis that allows us to do so.

Please note that we may process your or your child's personal information without your knowledge or consent in compliance with the above rules where this is required or permitted by law.

3.1 Use of your personal data for marketing purposes

Where you have given us consent to do so, we may send you information by email or text promoting school events, campaigns, charitable causes or services that may be of interest to you.

You can withdraw consent or 'opt out' of receiving these emails and/or texts at any time by sending an 'Unsubscribe' message to office@cobhammontessori.co.uk

3.2 Use of your or your child's personal data in automated decision-making and profiling

We do not currently process any pupils' personal data through automated decision-making or profiling. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

3.3 Use of your child's personal data for filtering and monitoring purposes

While your child is in our school, we will monitor their use of our information and communication systems, equipment and facilities (e.g. school computers, tablets, and internet access). This is a statutory requirement under **Keeping Children Safe in Education (KCSIE) 2026**.

Why we monitor:

- To comply with our safeguarding duties and protect your child's welfare
- To identify safeguarding risks, including online risks such as cyberbullying, inappropriate content, or contact with harmful individuals
- To comply with health and safety and other legal obligations
- To ensure compliance with our policies (e.g. Safeguarding and Child Protection Policy, Online Safety Policy, ICT and E-Safety Policy, Acceptable Use Policy)
- To keep our network(s) and devices safe from unauthorised access and prevent malicious software from harming our systems

What we monitor: We use filtering and monitoring systems that:

- Block access to harmful or inappropriate content
- Monitor and record online activity on school devices and networks
- Alert designated staff to potential safeguarding concerns

How monitoring information is used: Information from monitoring systems may be:

- Reviewed by our Designated Safeguarding Lead (DSL) and other authorised staff
- Used to inform safeguarding responses and interventions
- Shared with parents/carers where appropriate
- Shared with external agencies (such as police or children's social care) where necessary to protect a child

Your child's privacy: We balance our monitoring obligations with your child's right to privacy. Monitoring is proportionate, necessary for safeguarding purposes, and conducted in accordance with data protection law.

Review of filtering and monitoring: Our filtering and monitoring systems are reviewed **at least once every academic year** by our Senior Leadership Team, supported by our DSL and IT support, to ensure they remain effective and appropriate.

3.4 Use of artificial intelligence (AI)

We may use artificial intelligence (AI) tools to support teaching, learning, and school operations. When we use AI tools that process your or your child's personal data, we ensure:

- The AI tool complies with UK data protection laws
- Appropriate safeguards are in place to protect personal data
- We have assessed the risks and benefits of using the AI tool
- We remain accountable for decisions made with AI support

AI and safeguarding:

We are aware of safeguarding risks associated with AI, including:

- AI-generated or altered images (e.g., deepfakes) that may be used to create nudes or semi-nudes
- Inappropriate content generation
- Privacy concerns

If we become aware of any incidents involving AI-generated or altered images of your child, we will treat this as a safeguarding concern and respond in accordance with our Safeguarding and Child Protection Policy.

Your rights:

You have the right to:

- Be informed when AI is used to process your or your child's personal data
- Object to automated decision-making (where decisions are made solely by AI without human involvement)
- Request human intervention in automated decision-making processes

For more information about our use of AI, please see our Data Protection Policy or contact our Data Protection Officer (see Section 10).

4. Our lawful basis for using this data

Our lawful bases for processing your or your child's personal data for the purposes listed in section 3 **Our lawful basis for using this data**

We will only process your or your child's personal data when we have a lawful basis to do so under UK data protection law. The lawful bases we rely on are:

Public task – The processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law. We rely on this basis when:

- Providing education to your child
- Safeguarding and promoting the welfare of children
- Complying with statutory requirements (e.g. school census, attendance records, reporting safeguarding concerns)
- Facilitating the efficient operation of the school

Legal obligation – The processing is necessary to comply with the law (not including contractual obligations). We rely on this basis when:

- We are legally required to share information with third parties (e.g. local authority, Department for Education, police, courts)
- We must comply with statutory data collection requirements (e.g. school census)
- We are required to report safeguarding concerns to children's social care or police

Contract – The processing is necessary for a contract with you or to take steps at your request before entering into a contract. We rely on this basis when:

- Processing fee payments and financial information
- Administering your child's place at the school in accordance with our terms and conditions

Vital interests – The processing is necessary to protect someone's life. We rely on this basis when:

- We need to use personal data in a life-or-death situation (e.g. medical emergency)

Consent – You have given us clear consent to process your or your child's personal data for a specific purpose. We rely on this basis when:

- Sending you marketing communications about school events or services
- Using photographs or videos of your child for promotional purposes (e.g. on our website, in our prospectus, on social media)
- Processing data for purposes that are not covered by another lawful basis

Where you have provided us with consent to use your or your child's data, you may withdraw this consent at any time by contacting us (see Section 10).

Legitimate interests – The processing is necessary for our legitimate interests or the legitimate interests of a third party, provided your or your child's interests and fundamental rights do not override those interests. We rely on this basis when:

- Promoting the objects and interests of the school (e.g. fundraising, alumni relations)
- Ensuring the school is well managed and protecting the school's reputation
- Protecting the school's financial interests
- Using information in connection with legal disputes
- Investigating complaints or concerns

When we rely on legitimate interests, we will always balance our interests against your or your child's rights and freedoms, and we will only process data where the impact on privacy is minimal.
In practice, the conditions we most commonly rely on for processing special category data are:

- **Substantial public interest** (safeguarding and protecting children)
- **Health or social care purposes** (managing medical conditions, administering medication, supporting pupils with SEND)
- **Explicit consent** (where appropriate, such as for sharing photographs or videos)

5. Collecting this data

We will only collect and use your and your or your child's information when the law allows us to as detailed above in section 4 of this notice. While the majority of information we collect about your or your child is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

We collect parent and pupil information from a number of sources including:

Information which you provide to us such as: Registration Forms, New Starter Forms, Confirmation of Sessions Forms, Medical and Care Plans, Consent Forms; Childcare payment details, Early Years Funding Forms, Medical Reports; Data relating to any Information which you share with us in writing or orally.

Information which we create such as: Daily observations of children; Photographic and video records of children's work; Samples of children's work; Written formative assessment reports; Written Summative Assessment Reports; Records of Accidents and Behavioural Incidents; Records of Administration of Prescribed Medicine; Attendance and Absence Records; Restrictive Intervention Records; References for other schools; Individual Support Plans; Records of meetings; Lesson Plans and Transparent Classroom records.

Information from Third Parties: We may receive information from Third Parties related to your child or family circumstances including from the Local Authority, Former Schools, Government Departments, Police Forces, Social Care and Medical professionals.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

6. How we store this data

We keep personal information about your child while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary to comply with our legal obligations or to meet our regulatory requirements. Our Data Retention Policy sets out how long we keep information about pupils. This is available on our website.

We have put in place appropriate security measures to prevent your or your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your child's personal data securely when we no longer have a legal requirement to retain it.

6.1 Data breaches

We take the security of your and your child's personal data very seriously. We have put in place appropriate technical and organisational measures to prevent personal data from being accidentally lost, used, accessed, altered, or disclosed in an unauthorised way.

What happens if there is a data breach:

If we become aware of a data breach that is likely to result in a risk to your or your child's rights and freedoms, we will:

- Report the breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it
- Notify you without undue delay if the breach is likely to result in a high risk to your or your child's rights and freedoms
- Provide you with information about the nature of the breach, the likely consequences, and the measures we are taking to address it

For more information about how we manage data breaches, please see our Data Breach Policy.

7. Who we share data with

We do not share information about your child with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required or necessary (and it complies with UK data protection law), we may share personal information about your child with:

- Schools that your child may attend after leaving us
- Our local authority, Surrey County Council – to meet our legal obligations to share certain information with it, such as safeguarding concerns, Early Years funding and information about exclusions
- Government departments or agencies
- Youth support services provider
- Department for Education
- Our regulator, [e.g. Ofsted]
- Suppliers and service providers:
- External education providers such as Bikeability, Painshill Trust
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Local Authority Designated Officer (LADO) – when managing allegations against staff
- Multi-agency safeguarding arrangements – including safeguarding partners (local authority, police, health services)
- Independent Inquiry into Child Sexual Abuse (IICSA) or any successor inquiry – if required (note: IICSA concluded in 2022, but records may still be subject to future inquiries)
- Filtering and monitoring system providers – to enable safeguarding monitoring of online activity
- Cloud storage providers – where we use cloud-based systems to store personal data (e.g. Transparent Classroom)

7.1 Sharing data with the Department for Education (DfE)

The Department for Education (a government department) collects personal data from schools and local authorities via various statutory data collections. We are required to share information about our pupils with the

The data is transferred securely and held by the Department for Education under a combination of software and hardware controls that meet the current government security policy framework.

The data we share with the DfE is used for a number of purposes, including to:

- Inform funding
- Monitor education policy and school accountability
- Support research

The information shared with the DfE could include:

- Your or your child's name and address
- Gender or ethnicity
- Details of any special educational needs (SEN)
- Details of schools attended
- Absence and exclusion information
- Information relating to exam results
- Information relating to any contact with children's services
- What they did after they finished school

Please note: this list is not exhaustive.

National Pupil Database (NPD)

We are required to provide information about pupils to the DfE as part of statutory data collections such as the school census and early years census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the DfE and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The DfE may share information from the NPD with third parties, such as other organisations that promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the DfE's webpage on how it collects and shares personal data.

You can also contact the Department for Education with any further questions about the NPD.

7.2 Transferring data internationally

We may share personal information about you or your child with international third parties, where different data protection legislation applies.

Transparent Classroom (United States)

We use Transparent Classroom, based in the United States, to plan and record progress about your child's learning and development, including video images.

When transferring personal data to the United States, we ensure appropriate safeguards are in place to protect your or your child's data, in accordance with UK GDPR requirements. These safeguards include:

- **Standard Contractual Clauses (SCCs)** approved by the UK Information Commissioner's Office
- Transparent Classroom's commitment to data protection standards (see their privacy policy: https://www.transparentclassroom.com/privacy?locale=en)
- Regular review of the security and data protection measures in place

We have assessed the risks of transferring data to Transparent Classroom and are satisfied that appropriate safeguards are in place.

Your rights regarding international transfers:

You have the right to ask us for more information about the safeguards we have put in place to protect your or your child's personal data when it is transferred internationally. Please contact our Data Protection Officer if you would like further information (see Section 10).

8. Your rights

8.1 How to access personal information that we hold about your or your child

You have a right to make a 'subject access request' to gain access to personal information that we hold about your or your child.

If you make a subject access request, and if we do hold information about your or your child, we will (subject to any exemptions that apply):

- Give you a description of it
- Tell you why we are holding it, how we are processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your or your child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your child for you to make a subject access request on their behalf.

We will respond to your subject access request **without undue delay and within one month** of receiving your request. If your request is complex or we receive multiple requests from you, we may extend this period by a further two months. If we need to extend the timeframe, we will inform you within one month of receiving your request and explain why the extension is necessary.
We will provide the information **free of charge**. However, if your request is manifestly unfounded or excessive (for example, because it is repetitive), we may charge a reasonable fee or refuse to respond.

8.3 Your other rights regarding your or your child's data

Under UK data protection law, you have certain rights regarding how your or your child's personal data is used and kept safe. For example, you have the right to:

- Object to our use of your or your child's personal data
- Object to the processing of your or your child's personal data that is likely to cause, or is causing, damage or distress
- Prevent your or your child's data being used to send direct marketing
- Object to and challenge the use of your or your child's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected or blocked
- In certain circumstances, have the personal data we hold about your or your child deleted or destroyed, or restrict its processing
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your or your child's personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the data protection regulations

We may refuse your information rights request for legitimate reasons, which depend on why we're processing it. Some rights may not apply in these circumstances:

- Your right to have all personal data deleted or destroyed doesn't apply when the lawful basis for processing is legal obligation or public task
- Your right to receive a copy of your personal data, or have your personal data transmitted to another controller, does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests
- Right to object to use of your private data doesn't apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't haven't the right to object, but you have the right to withdraw consent

See information on types of lawful basis in section 4 of this privacy notice.

To exercise any of these rights, please contact us (see 'Contact us' below).

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your child for you to make these requests on their behalf.

9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concerns about our data processing, please raise this with us in the first instance. You can make a complaint to us at any time by contacting Shona Dolan: shonadolan@cobhammontessori.co.uk

ternatively, you can make a complaint at any time to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/make-a-complaint/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

10. Contact us

If you have any questions or concerns, or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

Shona Dolan shonadolan@cobhammontessori.co.uk