

Cobham Montessori School

Education for life

Data Protection Policy

Contents

1.0 The GDPR.....	p.2
1.1 What is the point of the GDPR?	p.2
1.2. Who does it apply to?.....	p.2
1.3 What is Data?.....	p.2
2.0 The key principles of the GDPR.....	p.2
2.1 Lawfulness, transparency and fairness.....	p.2
2.2 Collect data for a specific purpose and use it for that purpose	p.2
2.3 Limited collection.....	p.2
2.4 Accuracy	p.2
2.5 Retention	p.2
2.6 Security.....	p.2
3.0 Data subjects.....	p.3
3.1 Data subjects' rights.....	p.3
4.0 Subject Access Requests	p.3
5.0 Who is a 'data controller'?.....	p.3
6.0 Who is a 'data processor'?	p.3
7.0 Processing data	p.4
8.0 Data Sharing	p.4
9.0 Breaches & Non Compliance.....	p.4
10.0 Consent.....	p.4
11.0 Consent and Renewal	p.5
12.0 For Pupils and Parents/Carers.....	p.5
13.0 Pupil Consent Procedure	p.5
14.0 Withdrawal of Consent.....	p.5
15.0 Data Protection Officer	p.5
16.0 Physical Security.....	p.5
17.0 Secure Disposal	p.6
18.0 Complaints & the Information Commissioner Office (ICO).....	p.6
19.0 Review	p.6

<https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>

1.0 The GDPR

The General Data Protection Regulation (GDPR) is a European Directive that was brought into UK law with an updated Data Protection Act in May 2018. Brexit has not changed it. The Data Protection Act 1998 was repealed and replaced with the Data Protection Act 2018.

1.1 What is the point of the GDPR?

The GDPR and new DPA exist to look after individuals' data. It is a series of safeguards for every individual. Information about individuals' needs to be treated with respect and be secure. The GDPR exists to protect individual rights in an increasingly digital world.

1.2. Who does it apply to?

The GDPR applies to everyone, including schools. Schools have more obligations than some small businesses. It is mandatory to comply with the GDPR.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and in accordance with the law.

1.3 What is Data?

Data is any information that relates to a living person which identifies them. This can be their name, address or phone number, for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEN or health needs. Information about other family members may also be on the school file.

2.0 The key principles of the GDPR

2.1 Lawfulness, transparency and fairness.

School must have a legitimate reason to hold the data; we explain this in the Data Privacy Notices on the website. We often ask for consent to use data about a pupil for a particular purpose. If a parent wishes to withdraw consent this can be done at any time. There are sometimes when you cannot withdraw consent as explained in 'Data Subjects' Rights' (Clause 3.1).

2.2 Collect data for a specific purpose and use it for that purpose

So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

2.3 Limited collection

Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.

2.4 Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. We do this when pupils join the school and check on an annual basis.

If a Data Subject feels that the information held is inaccurate, should no longer be held by the Controller or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed, using the suitable forms.

2.5 Retention

Cobham Montessori School has a Data Retention policy that explains how long we store records for.

2.6 Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information.

3.0 Data subjects

A data subject is someone whose details we keep on file. Some details are more sensitive than others.

3.1 Data subjects' rights

Individuals have a right:-

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns, sharing information for the prevention and detection of crime. Schools may also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases these obligations override individual rights.

4.0 Subject Access Requests

You can ask for copies of information that we hold about you or about a pupil of Cobham Montessori School for whom you have parental responsibility. This Subject Access Request process is set out separately. You need to fill out the form, and you may need to provide identification evidence for us to process the request.

We have to provide the information within a month, but this can be extended if, for example, the school was closed for holidays. The maximum extension is up to two months.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure you access what you need, rather than sometimes getting a lot of information that may not be relevant to your query.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, or in some cases you may be better to approach them directly, e.g. paediatric therapists who are employed by the NHS.

We will usually supply the information in an electronic form.

If you wish to complain about the process, please see our complaints policy and later information in this policy.

5.0 Who is a 'data controller'?

The Head of School is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.

6.0 Who is a 'data processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a peripatetic teacher, a third-party company, a contractor, a volunteer or temporary employee. It can also be another organisation such as the police or the LA.

Data controllers must make sure that data processors are as careful about the data as the controller themselves. The GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

7.0 Processing data

Cobham Montessori School must have a reason to process the data about an individual. Our privacy notices set out how we use data. The GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

If there is a data breach, we have a separate policy and procedure to follow to take immediate action to remedy the situation as quickly as possible.

The legal basis and authority for collecting and processing data in school are:-

- consent obtained from the data subject or their parent
- performance of a contract where the data subject is a party
- compliance with a legal obligation
- to protect the vital interests of the data subject or other associated person
- to carry out the processing that is in the public interest and/or official authority
- it is necessary for the legitimate interests of the data controller or third party
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child
- necessary to comply with employment rights or obligations
- protection of the vital interests of the data subject or associated person
- being necessary to comply with the legitimate activities of the school
- existing personal data that has been made public by the data subject and is no longer confidential
- bringing or defending legal claims
- safeguarding
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems other than payroll and pensions data which is recorded on the third party contractor's systems.

8.0 Data Sharing

Data sharing is done within the limits set by the GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

9.0 Breaches & Non Compliance

If there is non-compliance with the policy or processes, or there is a DPA breach as described within the GDPR and DPA 2018 then the guidance set out in the Data Breach Policy needs to be followed.

Protecting data and maintaining data subjects' rights is the purpose of this policy and associated procedures.

10.0 Consent

For certain data we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required and the bases for collecting and using these data are set out in the privacy notices. However, in other cases data will only be processed if explicit consent has been obtained.

Consent is defined by the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

11.0 Consent and Renewal

On the school website we have 'Privacy Notices' that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

12.0 For Pupils and Parents/Carers

On joining the school you will be asked to complete various forms giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the Registration forms, Confirmation of Sessions forms, Annual Information Update forms, Health Declaration forms and New Starter forms.

We review forms on an annual basis. It is important to inform the school if details or your decision about consent changes.

13.0 Pupil Consent Procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

14.0 Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of GDPR and also child welfare, protection and safeguarding principles.

15.0 Data Protection Officer

We have a Data Protection Officer whose role is:-

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations under the GDPR
- to monitor compliance with the GDPR and DPA
- to provide advice where requested about the (DPIA) data protection impact assessment and monitor its performance
- to be the point of contact for Data Subjects if there are concerns about data protection
- to cooperate with the supervisory authority and manage the breach procedure
- to advise about training and CPD for the GDPR.

Our DPO is Shona Dolan. Her contact details are:

Email: shonadolancobhammontessori.co.uk

16.0 Physical Security

In school, all staff are responsible for ensuring that physical records are securely maintained and access controlled if an area is unoccupied, i.e. locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The Head of School is responsible for authorising access to secure data along with the Data Protection Officer.

All Staff, contractors and third parties must take due care to prevent data breaches.

17.0 Secure Disposal

When disposal of items is necessary a suitable process must be used. This is to secure the data, to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to ensure GDPR and DPA compliance.

Paper copies are shredded using a cross-cut shredder.

18.0 Complaints & the Information Commissioner Office (ICO)

The school Complaint Policy deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked to us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations.

Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

19.0 Review

A review of the effectiveness of GDPR compliance and processes will be conducted by the Data Protection Officer every 12 months.

This policy will also be reviewed if and when any new local or national guidance for schools is published.