



UK GENERAL DATA PROTECTION REGULATION (UK GDPR) POLICY

The UK General Data Protection Regulation (UK GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. This includes both staff and children. How the Colourbox Montessori School Ltd. (The Company) obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, has the right to know how the information about them is used. The General Data Protection Regulation requires the Company to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by the Company will typically achieve this balance and help to comply with the legislation.

We will respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; in addition, the means of storing and sharing that information takes place within the framework of the UK General Data Protection Regulation and the Human Rights Act.

UK General Data Protection Regulation principles:

To comply with the act, the Company will observe the eight 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. (see Retention chart)
- Personal data shall be processed in accordance with the rights of data subjects under this Act.

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In practice, it means that the Company must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;

Individual Rights

The UK General Data Protection Regulation includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The UK General Data Protection Regulation entitles an individual the right to request the personal information a Company holds on their behalf – this is known as a Subject Access Request (SAR) and includes all and any information held by the Company, not just that information held on central files or electronically, so it could also include correspondence, notes or CCTV images held by others in the Company.

- SARs must be responded to within 1 month of receipt.
- The SAR should be made in writing by the individual making the request.
- The Company can refuse or charge for requests that are manifestly unfounded or excessive
- Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Staff Responsibilities

Staff need to know and understand:

- How to manage, keep and dispose of data
- The Company's procedures in relation to children's records, email, social media, taking photos in the Company, mobile technology and the Company website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

Computer Access Control – Individual's Responsibility Access to the Colourbox Montessori IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Colourbox Montessori School Ltd. IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any Colourbox Montessori School IT system
- Leave their user accounts logged in at an unattended and unlocked computer
- Use someone else's user ID and password to access Colourbox Montessori School IT systems
- Leave their password unprotected (for example writing it down)
- Attempt to access data that they are not authorised to use or access
- Exceed the limits of their authorisation or specific business need to interrogate the system or data
- Store Colourbox Montessori data on any non-authorised Colourbox Montessori equipment
- Give or transfer Colourbox Montessori data or software to any person or organisation outside Colourbox Montessori without the authority of Colourbox Montessori School Ltd

Actions upon Termination of Contract:

All Colourbox Montessori School Ltd. equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Colourbox Montessori School Ltd. at termination of contract. All Colourbox Montessori School Ltd. data or intellectual property developed or gained during the period of employment remains the property of Colourbox Montessori School Ltd. and must not be retained beyond termination or reused for any other purpose.

Legal Framework General Data Protection Regulation 2018 <https://ico.org.uk/> Data Protection Act 1998 Computer Misuse Act 1990 Freedom of Information Act 2000 Human Rights Act 1999 The Children Act 2004, 2006 (Every Child Matters) Statutory Framework Statutory Framework for the Early Years Section 3: The Safeguarding and Welfare requirements 3.67- 3.72 Guidance Please see separate Child Protection Policy.

This policy will be reviewed in April 2023