



## Standard Operating Procedure

### DCS, MOD Schools, Early Years Settings

#### Standard Operating Procedure (SOP): GDPR, Information Management and Data Protection

Written by: Anita Collins

Date written: 10/08/2021

Reviewed Date: 23/08/2023

#### 1. Purpose

To ensure that all personal data collected about staff, children, parents, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

#### Definition/ Personal data;

Any information relating to an identified, or identifiable, individual.

This may include the individual's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

#### 2. Procedure

- All staff must understand that personal data is not only 'private' information. Personal data can include information that is already in the public domain. Anything that can be used alongside another piece of information to identify a living individual is considered personal data.



- Personal data should be anonymised when not stored securely. An example would be not including children's full names on photographs.

The five essential considerations in relation to GDPR are:

1. **Consent.** The individual has given clear consent for you to process their personal data for a specific purpose.
  2. **Contract.** The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
  3. **Legal Obligation.** The processing is necessary for you to comply with the law (not including contractual obligations).
  4. **Public Task.** The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
  5. **Legitimate Interests.** The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks.
- This information is issued in accordance with the guidance from the Information Commissioners Office (ICO). More information can be found at

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

### 3. Responsible Persons

- Data Controller - A controller is the person that decides how and why to collect and use the data (Usually the Manager/Deputy Manager).
- Data Processor – Anyone whom processes personal data is considered a 'processor'. An example would be administrators processing children's information for the purpose of raising invoices. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

#### All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this procedure
- Informing the setting/manager of any changes to their personal data, such as a change of address
- Contacting the manager in the following circumstances:



- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

#### **4. Responsibilities**

- Manager (Data Controller) to ensure annual GDPR audit is completed to document and record whom has access to personal data and the reason why.
- Staff (Data Processors) to ensure any personal data they have in paper form or digitally is deleted/destroyed when they no longer have a reason to store the information or in accordance with the annual review of records and safe data destruction.

#### **5. Directives**

- Record Management 7.1.2