



Data Protection Policy

GDPR-101

(V1.05)

Last review date:	13.04.2026
Next review date:	April 2027
Person/s responsible:	Miss C.Latimer

Version: 1.05

Release date: April 2026

Review date: April 2027

Contents

1. Aims	3
2. Legislation and Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Data Protection Principles	4
6. Roles and responsibilities	4
7. Subject Access Requests	6

8.Data Accuracy.....	7
9.Biometric recognition	7
10.Storage of records	7
11.Disposal of Records	8
12. Contact information	10

1. Aims

Centre of Education aims to ensure that all data collected about staff, students, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR).

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

2. Legislation and Guidance

This policy meets the requirements of Data Protection Legislation, and is based on [guidance published by the Information Commissioner’s Office](#) and [model privacy notices published by the Department for Education](#);

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)

[Data Protection Act 2018 \(DPA 2018\)](#)

This policy is based on guidance published by the Information Commissioner’s Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

This policy also covers requirements of [Keeping Children Safe in Education 2023 \(KCSIE 2023\) paragraphs 141 and 142 Filtering and Monitoring](#).

It also reflects the ICO’s [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy complies with [regulation 5 of the Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child’s educational record.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified

Sensitive personal data	Data such as: <ul style="list-style-type: none"> • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording, storing, altering or destruction data
Data subject	The living individual whose personal data is held or processed
Data controller	A person or organisation that determines the purpose for which, and the way personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

Centre of Education processes personal information relating to students, staff, emergency contacts and visitors, CV's, DBS, and safeguarding checks and, therefore, is a data controller.

5. Data Protection Principles

The UK GDPR is based on the following data protection principles, or rules for good data handling:

- Data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and

organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Roles and responsibilities

Centre for Education has overall responsibility for ensuring that they comply with the obligations under the UK GDPR.

Day-to-day responsibilities rest with the Director. The Director will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform Centre of Education of any changes to their personal data, such as a change of address.

Data breach reporting is mandatory under the UK GDPR and all staff are aware of their obligation to report data breaches without delay.

6.1 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, Centre of Education. The purpose of processing this data is to assist in the running of the agency, including to:

- enable individuals to be paid
- facilitate safer recruitment practice
- support the effective performance management of staff
- improve the management of workforce data across the education sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable monitoring of people with, and without, Protected Characteristics under the Equality Act

Staff personal data includes, but is not limited to, information such as:

- contact details, next of kin
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics/protected characteristics
- medical information
- outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. This may include advisers such as our Occupational Health and our Human Resources advisers.

We are required, by law, to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the Headteacher.

7. Subject Access Requests

Under the UK GDPR, Staff have a right to request access to information the school holds about them. This is known as a Subject Access Request (SAR).

Subject Access Requests must be submitted in writing, either by letter or email. Requests should include:

- The subjects name
- A correspondence address
- A contact number and email address
- Details about the information requested

The agency will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

8. Data Accuracy

Data Held will be as accurate and up to date as it reasonably possible. If a data subject informs the agency of a change of circumstances hir/her computer records will be updated as soon as is practicable.

Where a data subject challenges the accuracy of his/her data the agency will immediately mark the record as potentially inaccurate, or "challenged". In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the formal complaint's procedure.

9. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information should not be left in an office or on desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the office. Staff must adhere to policies and procedures when taking data off site.

- Passwords that are at least 8 characters long containing letters and numbers are used to access computers, online resources, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Encryption, anonymisation and pseudonymisation will be used to protect the data.
- Staff who store personal information on their personal devices are expected to follow the same security procedures for agency-owned equipment.
- UK GDPR compliant cloud storage will be used for all online data storage.

10. Disposal of records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely according to the Data Destruction Policy.

For example, we will shred or incinerate paper-based records and override electronic files. We also use an outside company to convert paper records to electronic and to shred documents on site.

11. Storage of records

The Director is responsible for monitoring and reviewing this policy.

The Director checks that the agency complies with this policy by, among other things, reviewing records at least annually or more frequently if required.

This document will be reviewed when the General Data Protection Regulation comes into force, and then **every year**.

At every review, the policy will be shared with the Governing Body.

12. Contact

If you would like to discuss anything in this privacy, In the first instance please contact the Director below:

Position	Name	Email	Phone
Director	Caitlin Latimer	Caitlin@centreofeducation.co.uk	07487601018