CVSE Data Protection Policy

Authors	Personnel
Policy Lead	Kate Lunn
Date Ratified by the personnel team	March 2012
Status	Ratified
Last Review Date	Sep. 2025
Policy Number	CVSE doc 40

Data Protection Policy

Introduction

Calder Valley Steiner Education (CVSE) collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Setting (both Nursery and Stay and Play Groups) in order provide assurances for education and associated functions. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LEAs), government agencies and other bodies.

The guidance in this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the GDPR 2018 and other related legislation. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Personal Data is defined as;
“Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Safeguarding and the welfare of the children will remain paramount.

CVSE Data protection officer is Kate Lunn

GDPR 6 Principles:

1. PROCESSED FAIRLY, LAWFULLY AND IN A TRANSPARENT MANNER as Data Controllers, you have to ensure that the personal data you are collecting, storing, using, sharing or processing in any way is being done so fairly and lawfully. You must have a legal basis for using the data and have made sure the data subjects are aware of the fact that you are using their data.
   You must understand: •
- what personal data you are using
    - what specific purpose you are using it for
    - If it is to be shared, details of who it is to be shared with (name of the company/supplier etc.) •
- How long it will be stored for and/or processed •

- The identity of the Data Controller (usually the school, but in Scotland the local authority) •
- Name and contact details of the Data Protection Officer
    - Their subject rights and how to exercise these.

2. USED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

This means that once you have explained to the data subject what data you are using and why, you cannot then decide to use that data for another purpose without first making them aware of this. It also means that you cannot use any form of 'blanket' basis for processing. In other words, you can't simply say that you are going to use their data for whatever the school needs.

3. USED IN A WAY THAT IS ADEQUATE, RELEVANT AND LIMITED

What is meant here is that you should ensure you use as much personal data as is required for the specific purpose and no more, especially if you are sharing pupil's personal data with a school supplier.

4. ACCURATE AND KEPT UP-TO-DATE

The personal data must be accurate when it is obtained – the school will endeavor to check personal data held on file on a regular basis.

5. KEPT NO LONGER THAN IS NECESSARY

Personal data must only be retained as long as it is required for the processing specified. Once it is no longer needed it should be securely erased unless there is a legitimate reason to keep it – such as legal requirements, the need to retain financial records etc.
In secondary schools, guidelines suggest that the majority of pupil data should be retained until the pupil reaches 25 years of age, except in special circumstances. In primary schools, guidelines suggest that the data should be retained whilst the pupil is attending the school and then should move with the pupil to their next educational establishment.
In schools, there needs to be a clear data retention policy which is adhered to but unfortunately there are often large amounts of personal data that are retained within administrative software well beyond the guidelines.

6. PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF THE DATA

Personal data has to be protected against unauthorized or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures.

The CVSE is committed to maintaining those principles at all times.
This means that the CVSE will:

- tell you what purposes we will use information for when we collect it
- if information will be shared, we will tell you why, with whom and under what circumstances
- check the quality and accuracy of the information we hold
- apply our records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorized for disposal it is done appropriately
- ensure appropriate security measures to safeguard personal information whether that is held in paper files or on our computer system, filing cabinets will be locked and the computer will be password protected.
- share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access in the Data Protection Act
- train our staff so that they are aware of our policies and procedures
- there is a separate photo consent policy available
- Parents are requested to not take photos of other children (than their own) without permission either on a mobile or camera.
- CVSE will be registered with the ICO.
- CVSE will use a first name only on registers where possible
- CVSE will obtain written consents
- CVSE will review all current paperwork to ensure only necessary information is collected.

This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act 1998.

Complaints
Complaints regarding this policy should be made to the Setting Manager who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the CVSE complaint procedure should be forwarded in writing to the Board of Trustees.

Contacts
If you have any concerns or questions in relation to this policy please contact the CVSE Manager, who will also act as the contact point for any requests under the GDPR.

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk

Dealing with a Data Protection Request

1. A request under the GDPR must be made in writing.
2. CVSE will respond to the request within 20 school days or 60 working days. (whichever is shorter), unless there are mitigating circumstances, at which time CVSE will inform the parent of the delay
3. CVSE needs time to redact other children's names on documentation
4. In many cases a letter to the Setting Manger will be sufficient to identify the information required. If you cannot identify the information required from the initial request you can go back to the applicant to ask for more information.
5. The Setting Manager must be confident of the identity of the individual making the request. This could be done by checking signatures against verified signatures on file or by asking the applicant to produce valid identification, such as a passport or photo-driving license. These checks should be done in addition to proof of relationship with the child.
6. An individual only has the automatic right to access information about themselves, requests from family members, carers or parents of a minor will have to be considered. The Setting Manager will have responsibility for ensuring the child's welfare is appropriately considered in deciding whether to comply with a request. Normally the requester will have to prove both their relationship with the child and that disclosure is in the child's best interests to the satisfaction of the Setting Manager. (In the event of a child having sufficient capacity to understand (normally age 12 or above) the Chair of College should discuss the request with the child and take their views into account when making a decision**.** There may be circumstance in which a child can refuse their consent to a request.)
7. CVSE may charge a statutory fee to cover printing and administration costs, currently calculated on a sliding scale, but only if a permanent copy of the information is provided. If a letter is sent out requesting a fee the 40-calendar day statutory timescale does not begin until the fee is received. It is important though that no request is delayed unnecessarily by time taken to inform the applicant of a fee. This is an administration charge.
8. CVSE will make use of exemptions under the GDPR as appropriate. All files must be reviewed before any disclosure takes place. **Under no circumstance will access be granted immediately or before this review process has taken place.**

Complaints

Complaints about the operation of these procedures should be made to the Board of Trustees who will decide if it is appropriate for the compliant to be dealt with under the complaint's procedure. Complaints which are not dealt with under the CVSE complaint procedure should be forwarded in writing to the Information

Commissioner. It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the Governing Body, complaints that involve consideration of personal data or sensitive personal data should be referred to the Information Commissioner.

Contacts

If you have any concerns or questions in relation to this policy please contact the Setting Manager, who will also act as the contact point for any requests under the GDPR.

Related Policies

- CVSE Privacy Policy

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk