East Bergholt
CEVC Primary School

'I have come that they might have life, and have it to the full' John 10:10

GDPR Policy
2026-2027

Prepared by:	Clare Sampson Headteacher
Approved by:	Full Governing Body
Signature of Chair of Governors:	Chris Burns
Date approved:	January 2026
Review date:	January 2027

Contents

Part 1 - Introduction and Key Definitions

1.1 Introduction

East Bergholt CEVC Primary School collects and processes personal data relating to pupils, parents and carers, staff, governors, volunteers, suppliers and other individuals with whom the school has a relationship. This information is necessary to enable the school to carry out its functions effectively, safely and in the public interest.

This Data Protection Policy sets out how the school collects, uses, stores, shares and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018**.** It also reflects guidance issued by the Information Commissioner's Office (ICO) and relevant expectations for schools.

This policy ensures that East Bergholt CEVC Primary School:

- complies with data protection legislation and regulatory guidance
- protects the rights and freedoms of pupils, staff, parents and carers
- is transparent about how personal data is processed
- has appropriate measures in place to protect personal data from misuse, loss or unauthorised access
- meets its accountability obligations as a data controller

The school processes personal data in line with the UK GDPR principles, which require that personal data is:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- retained only for as long as necessary
- processed securely, protecting against unauthorised or unlawful processing, accidental loss, destruction or damage

As a public authority, the school generally processes personal data under the lawful bases of legal obligation and public task**.** Consent is used only where appropriate and where a genuine choice exists**,** such as for the use of photographs or participation in optional activities.

Children's personal data is afforded particular protection. The school recognises its responsibility to handle pupil data with care, applying appropriate safeguards and ensuring that information is shared only where lawful, necessary and proportionate, including where required to safeguard children.

1.1 Key Definitions

Data

The DPA describes how organisations, including East Bergholt CEVC Primary School must collect, handle and store personal information ('data').

Data is any information that the school collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- 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.

Data can be stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Subject

A 'Data Subject' is someone whose details the school keeps on file. The data subject has the following rights under data protection legislation:

- to be informed
- to have access to data stored about them (or their children)
- to rectification if there is an error in the data stored
- to erasure if there is no longer a need for the school to keep their data
- to restrict processing (e.g. limit what their data is used for)
- to object to data being shared or collected

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc. override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf. The school is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff or a third party company such as a curriculum software provider or a payroll provider.

Part 2 Organisational Arrangements

2.1 Overall Responsibility

East Bergholt CEVC Primary School meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

The Governing Body will:

- Establish and maintain a positive data protection culture.
- Ensure the Headteacher prepares a Data Protection policy for approval and adoption by the governing body and to review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the school provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.
- Attend data protection training as organised by the school

The Headteacher will:

- Promote a positive data protection culture.
- Prepare a Data Protection Policy for approval by the governing body and revise as necessary and review annually

- Ensure that all staff co-operate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

The Data Protection Officer will:

- Inform and advise the school of their obligations under data protection legislation
- Monitor compliance with the legislation and report to the headteacer and governing body on a termly basis
- Co-operate with the supervisory authority (e.g. Information Commissioners Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioners Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools.
- Advise and guide the school on subject access requests and data breaches.

The Data Protection Lead:

- Act upon information and advice on data protection and circulate to staff and governors
- Carry out a data protection induction for all staff and keep records of that induction.
- Coordinate data protection training for staff and governors
- Coordinate the response to a Subject Access Request
- Coordinate the response to a data breach

Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy
- Comply with the school data protection arrangements.
- Follow the data breach reporting process
- Attend data protection training as organised by the school

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the school must register as a Data Controller on the Data Protection Register held by the Information Commissioner.

Data Protection Officer

As a public body, East Bergholt CEVC Primary School is required to appoint a Data Protection Officer (DPO).

At East Bergholt CEVC Primary School the DPO role is fulfilled by:

- Mrs Clare Sampson in conjunction with School Business Management Services (SBM)

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws.
- Monitor compliance with the relevant data protection laws.
- Be the first point of contact for supervisory authorities.

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school/academy).

Staff and governors/trustees will also be required to complete annual cyber security training to ensure that they are aware of cyber risks and understand the important role that they play in reducing the risk of a successful cyber-attack.

Annual data protection refresher training will take place to reinforce the importance of staff and governors adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping

East Bergholt CEVC Primary School has documented all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- how consent is obtained
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data
- how the data is shared
- how the data is destroyed

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the headteacher to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

Third Party Suppliers Acting as Data Processors

As Data Controller, the school is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all subcontractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- IT contracts and processes
- Physical data and hard copy documents
- Data destruction and hardware renewal and recycling financial and personnel information
- Pupil and staff records

Only third-party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners. The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract. The external processor will confirm with the data controller that

suitable security and operational measures are in place. Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of a data breach or subject access request, or enquiries from the ICO.

The school must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems. Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include cooperation and eventual secure destruction or return of data.

The school has a 'Third Party Request for Information' form which must be used for third-party suppliers acting as a Data Processor for the school.

The school maintains evidence of the checks that have taken place for each of their third party suppliers.

Consent

East Bergholt CEVC Primary School recognises that consent is not the primary lawful basis for processing personal data in schools. As a public authority, the school generally processes personal data under the lawful bases of legal obligation and public task, where processing is necessary to fulfil statutory duties and functions.

Consent is used only where appropriate and where a genuine choice exists, and where the processing is not required by law or necessary to carry out the school's public functions. Examples of where consent may be used include, but are not limited to, the use of pupil or staff photographs and videos, participation in optional activities, and the use of images or information for promotional or social media purposes.

Where consent is relied upon as the lawful basis for processing, it will be freely given, specific, informed and unambiguous, obtained through a clear affirmative action, and recorded and managed appropriately. The school will make clear to individuals why consent is being sought, how the data will be used, and that consent can be withdrawn at any time without detriment.

Consent will not be used where there is an imbalance of power, or where the school is required to process data as part of its statutory responsibilities, including education, safeguarding, attendance, assessment and reporting duties.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the school will inform their staff, parents/carers of all pupils and governors of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff, parents and governors through the following means:

- School website

- School newsletter
- School prospectus
- Letter to parents
- Staff Handbook
- Staff Notice Boards

Privacy notices will be reviewed on an annual basis.

The Use of Images (Pupil & Staff)

Occasionally the school may take photographs of its pupils or staff members. These images could be used as part of internal displays, printed publications, the website or our social media accounts. East Bergholt CEVC Primary School will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images.

Parents and staff are given the opportunity to opt in. It is not permissible to assume they are opting in. Generic consent for all uses of images is not acceptable; parents and staff must give consent to each medium.

Parents and staff must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school, however a verbal withdrawal of consent is also valid and should be reported to the headteacher immediately.

Consent should be recorded and will be logged on SIMS. If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

The school 'Parental Consent' and 'Staff Consent' forms are used to seek consent when they join the organisation.

Accurate Data

The school will endeavour to ensure that the data it stores is accurate and up to date. When a pupil or member of staff joins the school they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the school will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the school to use the information held for internal purposes.

Parents/carers and staff are requested to inform the school when their personal information changes.

Withdrawal of Consent

Where personal data is processed on the basis of consent, individuals have the right to withdraw that consent at any time. Withdrawal of consent will not affect the lawfulness of any processing carried out before consent was withdrawn.

Requests to withdraw consent should be made in writing to the school office. Verbal requests will also be accepted and acted upon appropriately. Once consent is withdrawn, the school will cease the relevant processing as soon as reasonably practicable, unless there is another lawful basis which permits or requires continued processing.

Where more than one person has parental responsibility, the school will consider each request on a case-by-case basis, acting in the best interests of the child and in line with safeguarding and data protection principles.

Associated Data Protection Policies

- Complaints
- ICT Usage Agreement
- Records Management & Retention
- Subject Access Requests

Complaints

Complaints will be dealt with in accordance with the school's Complaints Procedure. An individual may contact the Information Commissioner's Office (ICO) if they are not satisfied with how a complaint has been dealt with by the school. The telephone number for the ICO is 0303 123 1113.

Confidentiality Agreement

The school has a Confidentiality Agreement in place which staff, governors/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the school has in relation to maintaining confidentiality.

Data Breaches

Although the school takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone)
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the school

The school has a Data Breach policy which sets out the process that should be followed in the event of a data breach occurring.

Data Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the headteacher. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO should consult with the ICO prior to implementation.
The 'Data Privacy Impact Assessment' form must be used for each new service/product.

ICT Usage Agreements

The school has an ICT Usage Agreement in place which staff, governors/trustees and volunteers are required to sign on an annual basis. This agreement sets out the expectations the school has in relation to staff safely and securely using the IT network.

Records Management

The school recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

The school has a Record Management & Retention Policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

The retention schedule is based on the good practice advice provided by the Institute of Records Management Society (IRMS) for schools.

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school holds about them and can make a Subject Access Request (SAR). The school has a Subject Access Request Policy, which sets out how a SAR can be made and the process that should be followed in the event of receiving a SAR.

Third Party Requests for Information

Occasionally the school may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The school has a Third Party Request for Information Policy which sets out the process that should be followed in the event of receiving a third party request.

Use of Personal Devices

The school recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. The school follows the 'Bring Your Own Device' Policy which sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.