DATA PROTECTION POLICY

Capel St. Mary CEVC Primary School
The Street, Capel St Mary, Ipswich, Suffolk IP9 2EG
t 01473 310386

e:mail: admin@capel-st-mary.suffolk.sch.uk
website: www.capel-st-mary.suffolk.sch.uk

Care
Achieve
Persevere
Enjoy
Learn

Suffolk County Council

Part 1 Introduction and Key Definitions

1.1 Introduction

Capel St Mary CEVC Primary School ("Capel School") needs to gather and use certain information about individuals.

These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people Capel School has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the school's data protection standards — and to comply with the law.
This data protection policy ensures Capel School:

- complies with data protection law and follows good practice
- protects the rights of pupils, staff, parents/carers and other stakeholders
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

This Data Protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner
2. collected for specified, explicit and legitimate purposes
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. accurate and kept up to date
5. kept in a form which permits identification of data subjects for no longer than is necessary
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations, including Capel 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 on 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 Governing Body 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, third party company or another organisation such as the police or Local Authority (LA).

Part 2 Organisational Arrangements

2.1 Overall Responsibility

Capel School will 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.

The Headteacher will:

- Promote a positive data protection culture.
- Prepare a Data Protection policy for approval by the Governing Body, revise as necessary and review on an annual basis
- 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 Headteacher and governing body on a termly basis.
- Cooperate 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.
- 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 the school response to a Subject Access Request.
- Coordinate the school 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. The school was first registered on 15 September 2003 and is due to renew on 14 September 2026

Data Protection Officer

As a public body, Capel School is required to appoint a Data Protection Officer (DPO).

At Capel School the DPO role is fulfilled by:

SBM Services

The role of the DPO is to:

- Inform and advise the school 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.

Cyber security training for staff is included within safeguarding training which is delivered to all staff annually. This is 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.

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

Data Mapping

Capel 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 DPO to ensure the 'Data Flow Map' is kept up to date. The map should be a live document and updated regularly.

3.2 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 sub contractors 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 organizational 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 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 co-operation 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

3.3 Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, the school will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (eg 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
- Letter/email to parents
- Staff induction documentation

The Use of Images (Pupils and Staff)

Occasionally the school may take photographs of its pupils and staff members. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

When a child is registered at Capel School, we will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Parents are requested to do this via our Management Information System (MIS), Arbor.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents must give consent to each medium. Parents 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 Data Processor immediately.

Consent is recorded by the school office staff.

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.

At Capel St Mary CEVC Primary School, we sometimes take photographs / videos of staff. We use these photos for a range of purposes. For example, photos including staff members appear on our website, on internal displays and on social media to share information about school activities. Photos may be used on posters about employees' roles in school. These purposes for sharing photos are a necessary part of the school's work and this data is shared on the lawful basis of 'Public Task'.

We also use photos for marketing purposes, such as on advertisements and in our prospectus. On these occasions, we process images of staff members on the lawful basis of 'Legitimate Interests'. We value using staff photos, not only for transparency to parents as to identify who staff are, but also for ease of identification for safeguarding purposes and to celebrate the curriculum and enrichment opportunities in school.

If staff members wish to opt out of us using your images for any of the reasons mentioned above they may do so 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 Data Processor immediately.

Accurate Data

The school will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil joins the school they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number), 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).

When a member of staff joins the school, their application for employment will be used to provide contact details etc. A further Request of Next of Kin and Emergency details form is also completed.

The school will send an annual reminder to parents and staff to ask them to check the data that is held about them is correct. This exercise will also allow individuals the opportunity to review the consent they have given to the school previously.

Parents/carers and staff are requested to inform the school when their personal information changes. Parents/carers are also able to amend this information themselves by Arbor.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on the merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the Data Processor.

Complaints

If an individual believes the school has mishandled their personal data or that their data protection rights have been breached, they have the right to make a complaint.

Concerns or complaints should be directed as follows in the first instance to:

- Andrew Frolish (Headteacher)
- admin@capel-st-mary.suffolk.sch.uk
- 01473 310386

Complaints will be acknowledged by the school at the earliest opportunity, but at the latest within 30 days.

The school will take reasonable steps to investigate the concern without undue delay.

The individual that has raised the complaint will be informed of the outcome once the investigation has concluded.

If the individual is unsatisfied with how the complaint has been managed, they can escalate their concern to the Information Commissioner.

Website: Make a complaint about how an organisation has used your personal information | ICO

Phone: 0303 123 1113

3.4 Linked Data Protection Policies/Processes

- Confidentiality Agreement
- Data Breaches
- Data Privacy Impact Assessments
- Online Safety and Acceptable Use of Devices Policy
- Records Management & Retention
- Subject Access Requests
- Third Party Requests for Information
- Information sharing in an employee medical or mental health emergency

Confidentiality Agreement

The school has a Confidentiality Agreement in place which staff, governors and volunteers are required to sign. 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 DPO. 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 Online Safety and Acceptable Use of Devices Policy in place which staff, governors 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.

Information sharing in an employee medical or mental health emergency

Data protection law allows the school to share personal information in an urgent or emergency situation, including to help prevent loss of life or serious physical, emotional or mental harm.

During a medical or mental health emergency where there is risk of serious harm to staff or to others the school will share necessary and proportionate information without delay with relevant and appropriate emergency services or health professionals. The school may also share necessary and proportionate information with the member of staff's next of kin or emergency contact.

The school will use their judgement in each specific situation, sharing only what is necessary and proportionate to the circumstances. The school may decide that, whilst it may be necessary and proportionate to provide the emergency services with a full account of the situation, it is only appropriate to provide the member of staff's emergency contact with more limited details.

The school staff privacy notice covers this sharing of data.

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

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR).

The school has a Subject Access Request policy, which sets out 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. Staff follow the Online Safety and Acceptable Use of Devices Policy and are requested to complete and sign an Acceptable Use Agreement (Appendix 3 of the policy).

Review Date: February 2026
Next Review Date: February 2027