# CROCKERTON CHURCH OF ENGLAND VA PRIMARY SCHOOL

## VISION STATEMENT

Within the love of God together we live, learn, care, and celebrate.
For each other and for ourselves we aim for the best.

Potters Hill
Warminster
Wiltshire
BA12 8AB
Telephone: 01985 212168
Email: admin@crockerton.wilts.sch.uk
Website: https://crockerton.wilts.sch.uk/
Headteacher: Mrs N Ilic

# Data Protection and Security Policy

This is a single policy which has been written on behalf of the Governing Body for Crockerton Church of England VA Primary School.

| | |
|---|---|
| **Written** | March 2025 |
| **Reviewed** | |
| **Author** | DPO Officer & Governors |
| **Next Review** | March 2026 |

# Contents

## 1 Introduction

1.1 Crockerton Church of England VA Primary School (the school) is committed to protecting the personal data of our pupils, parents, staff, governors, and other stakeholders in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other relevant legislation.

1.2 This policy outlines our approach to managing personal data, including how we collect, use, store, and protect it. It also details the rights of individuals regarding their personal data and the procedures we have in place to ensure compliance.

## 2 Scope

2.1 This policy applies to all personal data processed by the school, regardless of format or medium. It covers data related to pupils, parents, staff, governors, volunteers, contractors, and other stakeholders.

2.2 This policy applies to all staff, including employees, volunteers, governors, and contractors, who process personal data on behalf of the school.

## 3 Biometric Data:

3.1 The School does not collect, store, or use biometric data for any purpose. Should this change in the future, the school will ensure compliance with all applicable data protection laws, including obtaining explicit consent from individuals or their parents/carers where required.

## 4 Key Definitions

- **Personal Data:** Any information relating to an identified or identifiable individual (data subject). This includes names, addresses, phone numbers, identification numbers, location data, and online identifiers.
- **Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation.
- **Processing:** Any operation or set of operations performed on personal data, including collection, storage, alteration, retrieval, use, disclosure, erasure, or destruction.
- **Data Controller:** The organisation that determines the purposes and means of processing personal data.
- **Data Processor:** A person or organisation that processes personal data on behalf of the data controller.

## 5 Data Protection Principles

5.1 The School adheres to the following data protection principles as outlined in the UK GDPR:

- **Lawfulness, Fairness, and Transparency:** Personal data must be processed lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data Minimization:** Data collected must be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased or rectified without delay.
- **Storage Limitation:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed.

- **Integrity and Confidentiality:** Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage.
- **Accountability:** The school must be able to demonstrate compliance with the above principles.

## 6 Lawful Basis for Processing

6.1 The School will only process personal data where we have a lawful basis for doing so. The lawful bases include:

- **Consent:** The individual has given clear consent for their personal data to be processed for a specific purpose.
- **Contractual Obligation:** Processing is necessary for a contract with the individual or to take steps before entering into a contract.
- **Legal Obligation:** Processing is necessary to comply with the law.
- **Vital Interests:** Processing is necessary to protect someone's life.
- **Public Task:** Processing is necessary to perform a task in the public interest or for official functions.
- **Legitimate Interests:** Processing is necessary for the legitimate interests of the school or a third party, provided the individual's rights and freedoms are not overridden.

## 7 Consent

7.1 Where consent is the lawful basis for processing personal data, it must be freely given, specific, informed, and unambiguous. The school will obtain explicit consent for the processing of special category data and for activities that require it, such as using photographs for marketing purposes.

7.2 Individuals have the right to withdraw consent at any time, and this will be communicated clearly at the point of consent collection.

## 8 Data Subject Rights

8.1 Individuals have the following rights concerning their personal data:

- **Right to be Informed:** Individuals have the right to be informed about the collection and use of their personal data.
- **Right of Access:** Individuals have the right to access their personal data and obtain a copy.
- **Right to Rectification:** Individuals have the right to have inaccurate personal data corrected.
- **Right to Erasure:** Individuals have the right to have their personal data erased in certain circumstances.
- **Right to Restrict Processing:** Individuals have the right to request the restriction of processing of their personal data.
- **Right to Data Portability:** Individuals have the right to receive their personal data in a structured, commonly used format and transfer it to another data controller.
- **Right to Object:** Individuals have the right to object to the processing of their personal data in certain circumstances.
- **Rights in Relation to Automated Decision-Making and Profiling:** Individuals have the right not to be subject to decisions based solely on automated processing.

8.2 The School will respond to any requests to exercise these rights within one month, in accordance with UK GDPR.

## 9 Data Security

9.1 The School implements appropriate technical and organisational measures to protect personal data against unauthorised access, disclosure, alteration, or destruction. These measures include:

- **Access Controls:** Restricting access to personal data to authorised personnel only.
- **Encryption:** Using encryption to protect personal data, particularly when transmitted over networks.

- **Data Breach Procedures:** Having procedures in place to identify, report, and manage data breaches promptly.
- **Regular Audits:** Conducting regular audits to assess the effectiveness of data protection measures.

## 10 Data Anonymisation and Pseudonymisation

10.1 The school is committed to using data anonymisation and pseudonymisation techniques where appropriate to minimise the risk to individuals' privacy. These methods are applied during the processing of personal data to ensure that individuals are not identifiable unless necessary for a specific purpose. The school reviews and updates its practices regularly to ensure compliance with UK GDPR and the Data Protection Act 2018.

## 11 CCTV Use:

11.1 Where used, the school uses Closed Circuit Television (CCTV) systems to support site security and safeguarding measures. The management and use of CCTV are governed by the school's CCTV Policy, which includes details about retention, access, and sharing. For more information, please refer to the CCTV Policy, available upon request.

## 12 Photograph and Video Consent

12.1 The school recognises the importance of protecting individuals' privacy when capturing and using photographs or videos. Consent is obtained from parents, carers, or pupils (where appropriate) before using images for any purpose. Detailed information on how the school manages and safeguards photographs and videos, including consent processes, is outlined in the Photograph and Video Policy, available on our website or upon request.

## 13 Bring Your Own Device (BYOD) Policy

13.1 The school permits staff to use personal devices for work purposes under strict conditions to ensure data protection and cybersecurity. All users must adhere to the BYOD Policy, which outlines acceptable use, security requirements, and responsibilities for safeguarding personal data accessed or stored on personal devices. The full policy is available on the school's website or upon request.

## 14 Data Breach Management

14.1 The School takes data breaches seriously and has a procedure in place for managing them. A data breach occurs when there is a security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

14.2 All staff are required to report any suspected data breach to the Data Protection Officer (DPO) immediately.

14.3 In the event of a data breach, the school will follow these steps:

- **Containment and Recovery:** The school will take immediate steps to contain the breach and recover any lost data.
- **Risk Assessment:** The school will assess the risks associated with the breach, including the potential impact on individuals.
- **Notification:** If the breach is likely to result in a high risk to individuals' rights and freedoms, the DPO, in collaboration with the school, will notify the affected individuals and the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.
- **Evaluation and Response:** The school will review the breach and take steps to prevent future incidents.

## 15 Data Retention and Disposal

15.1 The School will only retain personal data for as long as necessary to fulfil the purposes for which it was collected, in accordance with our Data Retention Schedule.

15.2 Personal data that is no longer required will be securely disposed of, whether through deletion, shredding, or other appropriate methods.

## 16 Data Protection Officer (DPO)

16.1 The School has appointed a Data Protection Officer (DPO) to oversee data protection matters and ensure compliance with the UK GDPR.

16.2 The DPO is responsible for:

- Monitoring compliance with data protection laws and policies.
- Advising on data protection obligations.
- Conducting data protection impact assessments (DPIAs).
- Acting as the point of contact for data subjects and the Information Commissioner's Office (ICO).

16.3 The DPO's contact details are as follows:

- Name: Jeremy Shatford
- Email: dpo@jeremyshatford.co.uk
- Phone: 07881297319

## 17 Training and Awareness

17.1 All staff, governors, and volunteers will receive regular training on data protection to ensure they are aware of their responsibilities and the school's policies and procedures.

17.2 The school will maintain records of training provided to staff and ensure that data protection is included in induction training for new staff members.

## 18 Data Protection Impact Assessments (DPIAs)

18.1 The School will conduct Data Protection Impact Assessments (DPIAs) for any new or significantly changed processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

18.2 The DPIA process will include:

- Identifying and assessing risks to data subjects.
- Consulting with the DPO and, where necessary, the ICO.
- Implementing measures to mitigate risks identified.

## 19 Third-Party Data Sharing Agreements

19.1 The school ensures that any sharing of personal data with third parties is governed by a written agreement that complies with UK GDPR and the Data Protection Act 2018. These agreements define the purpose, scope, and duration of data sharing, including appropriate security measures, and require third parties to process data in accordance with the school's instructions and legal requirements. Regular reviews are conducted to ensure compliance and continued adequacy of the agreements.

## 20 Policy Review

20.1 This Data Protection Policy will be reviewed annually or more frequently if necessary to reflect changes in legislation, guidance, or school practices.

20.2 Any updates to the policy will be communicated to staff, governors, volunteers, and other stakeholders as appropriate.

## 21 Contact Information

21.1 If you have any questions about this Data Protection Policy or your data protection rights, please contact our Data Protection Officer as above (11.3) or by contacting the school office whose details are above.