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 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	June 2026
Reviewed	
Author	DPO Officer & Governors
Next Review	June 2027

Data Protection Policy
Reviewed: June 2026
Next review: Annually

1 Introduction

1.1 Crockerton Ce Primary School ("the School") collects and processes personal data relating to pupils, staff, parents, and others in order to carry out its functions.

1.2 The School is a **Data Controller** under:

- UK GDPR
- Data Protection Act 2018
- Data Protection and Digital Information Act 2024 (DUAA)

1.3 The School is registered with the ICO.

- **Data Protection Officer (DPO):**
  Jeremy Shatford – dpo@jeremyshatford.co.uk

2 Purpose

2.1 This policy ensures that personal data is:

- Processed **lawfully, fairly and transparently**
- Used only for **specified purposes**
- **Adequate, relevant, and limited**
- **Accurate and up to date**
- Retained only as long as necessary
- Kept **secure**
- Fully **accountable**

2.2 This applies to all personal data in **electronic and paper formats**.

3 Governance and Responsibilities

3.1 Governing Body

- Overall accountability for compliance

3.2 Headteacher / Senior Leadership

- Ensure operational compliance

3.3 Data Protection Officer

- Advises, monitors, and reports on compliance

3.4 Staff

- Must follow this policy and all related procedures
- Must report concerns, risks, or breaches immediately

4 Data Protection Principles

4.1 The School complies with the UK GDPR principles:

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

5 Lawful Bases for Processing

5.1 The School processes data using:

- **Public Task** (main basis for education)
- **Legal obligation**

- **Contract**
- **Consent** (limited use)
- **Vital interests**
- **Legitimate interests** (where appropriate)

5.2 Special category data is processed under additional lawful conditions.

6 Rights of Individuals

6.1 Individuals have the right to:

- Be informed
- Access their data (SAR)
- Rectification
- Erasure (where applicable)
- Restrict processing
- Data portability
- Object
- Human review of automated decisions (including AI)

7 Data Sharing

7.1 Data is shared only where:

- There is a lawful basis
- It is necessary for safeguarding, education, or legal duties

7.2 The School ensures:

- Data Sharing Agreements where required
- Due diligence of all third parties

8 Information Security

8.1 The School implements:

- Access controls
- Encryption and secure systems
- Staff training
- Secure storage and disposal
- Alignment with NCSC and DfE guidance

9 Data Breaches

9.1 All breaches must be reported immediately.

9.2 The School will:

- Assess risk
- Record all breaches
- Notify ICO within 72 hours where required
- Inform individuals where necessary

10 Training and Awareness

- All staff receive induction and regular refresher training
- Compliance is monitored through audits and reviews

11 Related Documents

11.1 This policy is supported by:

- Data Protection Procedures Manual
- Subject Access Request Procedure
- Data Breach Procedure
- Retention Schedule
- Information Security / Acceptable Use Policy

DATA PROTECTION PROCEDURES MANUAL
(Operational guidance for staff)

1. Staff Responsibilities
All staff must:
- Handle personal data securely at all times
- Only access data necessary for their role
- Lock devices when unattended
- Use authorised systems only
- Never share passwords
- Report concerns or breaches immediately

2. Handling Personal Data
Staff must:
- Minimise data collected
- Ensure accuracy
- Follow retention schedules
- Store data securely
- Not retain data longer than necessary

3. Use of Devices
- Only school-approved devices should be used
- Personal devices must not be used for personal data unless authorised
- Devices must be password-protected and encrypted
- Data must not be stored locally unless necessary

4. Working Offsite
If data must be taken off-site:
- Only take what is necessary
- Keep data secure and out of sight
- Never leave data unattended in vehicles
- Return data promptly

5. Data Sharing
Staff must:
- Check lawful basis before sharing
- Use secure transfer methods
- Ensure recipient is authorised
- Seek advice if unsure

6. Third-Party Processors
Before engaging third parties:
- Confirm data protection compliance
- Ensure contracts are in place
- Limit access to necessary data only

7. Data Protection by Design
Before new activities:
- Consider privacy risks
- Conduct DPIA where required
- Consult DPO if needed

3. SUBJECT ACCESS REQUEST (SAR) PROCEDURE

Key Steps

1. Verify identity
2. Clarify the request if needed
3. Locate data using ROPA
4. Gather data from all sources
5. Review and redact
6. Provide securely within **1 month** (extend if complex) [Data Protection | PDF]

Key Rules

- Requests are usually **free**
- Extensions must be justified
- Keep audit trail

4. DATA BREACH PROCEDURE

When a breach occurs:

- **Staff must:**
- Report immediately to DPO or Data Lead
- **School will:**
- Contain breach
- Assess risk
- Record in breach log
- Notify ICO within 72 hours if required
- Inform individuals where necessary [Data Prote...March 2026 | Word]

5. INFORMATION SECURITY RULES (SHORT VERSION)

- Use strong passwords
- Lock screens (Windows + L)
- Do not share accounts
- Keep clear desks
- Dispose of data securely
- Be alert to phishing