**Policy Title: Data Protection & GDPR Policy**

**Date of Approval: October 2025**

**Approved By:**

| | |
|---|---|
| Andrew Orves | Oz Sparks |
| Chair of Governors | Headteacher |

**Policy Review Date:** October 2026 (or earlier if necessary)

**Policy Owner:** Headteacher

**Policy Statement:** *Carlton Colville Primary School is committed to complying with the UK GDPR and Data Protection Act 2018, ensuring all personal data is processed lawfully, fairly and transparently and is kept secure and confidential.*

**Related Documents:**

Privacy Notice

Safeguarding Policy

## 1 Purpose and scope

1.1 This policy sets out Carlton Colville Primary School's approach to the lawful, secure and confidential processing of personal data in line with the UK GDPR and the Data Protection Act 2018 and describes staff responsibilities for handling confidential information.

1.2 The policy applies to all personal and special-category data held by the school about pupils, parents/carers, staff, governors, volunteers and third parties in any format, including CCTV, audio and visual recordings, emails, paper records and electronic systems.

## 2 Policy statement

2.1 Carlton Colville Primary School is committed to processing personal data lawfully, fairly and transparently, ensuring data is accurate, kept for no longer than necessary, processed for specified purposes and secured against unauthorised access, loss, damage or destruction.

2.2 All staff, governors and third-party partners must treat personal and confidential information with strict confidentiality, use it only for authorised purposes and report any actual or suspected data breaches immediately.

## 3 Legal bases and data protection principles

3.1 The school will only process personal data where there is a valid legal basis, including consent, performance of a contract, legal obligation, vital interests, public task or legitimate interests where appropriate.

3.2 Processing will follow the GDPR principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

## 4 Roles and responsibilities

4.1 Governing Body: ensures appropriate policies, resources and oversight are in place and receives assurance that data protection obligations are met. 4.2 Headteacher: overall responsibility for implementing this policy and managing data protection risk.

4.3 Data Protection Lead / DPO (where appointed): provides advice, monitors compliance, handles DPIAs and is the contact for data subjects and the Information Commissioner's Office.

4.4 All staff, volunteers and governors: must follow this policy, attend required training, apply good data-handling practice and report incidents promptly.

## 5 Collection, use and disclosure of personal data

5.1 Personal data will be collected only for specified, explicit and legitimate purposes and will not be processed in a manner incompatible with those purposes.

5.2 Access to personal data will be limited to those with a genuine need to know. The school will not disclose personal data to third parties unless there is a lawful reason, including statutory requirement, data-sharing agreement or written consent.

5.3 Where information sharing is necessary to safeguard a child, staff must follow safeguarding procedures and lawfully share information with appropriate agencies.

**6 CCTV, recordings and images**

6.1 CCTV footage and other recorded images are personal data and are processed by the school under a lawful basis (typically legitimate interests or public task).

6.2 The school will ensure clear signage and publish information about CCTV use in privacy notices. Footage will be retained only for the minimum period necessary, access will be restricted, and disclosure will follow legal requirements.

6.3 Requests for access to footage will be treated as data subject access requests and handled in line with section 10 of this policy.

**7 Special category and safeguarding data**

7.1 Special category data and safeguarding records will be processed only where lawful and necessary, with additional safeguards applied. Access will be strictly controlled and limited to those with a demonstrable need.

7.2 Such records will be stored securely and retained only in line with statutory and local guidance.

**8 Records management, retention and disposal**

8.1 The school maintains a retention schedule that sets out retention periods for categories of records and secure disposal methods.

8.2 Staff must follow the retention schedule. If uncertain about retention or disposal, staff must consult the DPO or Headteacher before deleting or destroying records.

**9 Security, storage and transfer of data**

9.1 Personal data will be held securely in locked cabinets or on password-protected and encrypted IT systems. Access controls, strong passwords, encryption and physical security measures will be applied proportionately.

9.2 Staff must follow IT and security protocols for remote working, use of personal devices and email. Personal data must not be transferred outside the UK or EEA without appropriate safeguards.

**10 Data subject rights and subject access requests (SARs)**

10.1 Individuals have rights including access to their personal data, correction, erasure (in certain circumstances), restriction, objection to processing and data portability.

10.2 Requests should be made in writing to the DPO or via the school office. The school will verify identity and respond to valid requests without undue delay and within statutory timescales.

**11 Confidentiality, information sharing and permitted disclosures**

11.1 Confidential information must be treated with care; staff must not share confidential or personal data unless there is a lawful basis and a clear, documented reason.

11.2 Information will be shared where necessary to protect the welfare of pupils or to comply with legal obligations. All non-routine disclosures must be recorded, including the lawful basis and justification.

**12 Breach reporting and incident management**

12.1 All actual or suspected data breaches or confidentiality incidents must be reported immediately to the DPO and Headteacher. The school will investigate, contain and, where necessary, notify the Information Commissioner's Office and affected data subjects in line with statutory requirements.

12.2 Lessons learned from breaches will be applied to update practice and reduce future risk.

**13 Data Protection Impact Assessments (DPIAs)**

13.1 DPIAs will be carried out for high-risk processing activities or new systems that may impact individuals' privacy. DPIAs will be recorded, retained and used to inform risk mitigation.

**14 Third-party processors and contracts**

14.1 Where external organisations process personal data on the school's behalf, contracts will require processors to act only on the school's instructions and to implement appropriate technical and organisational measures. The school will carry out due diligence and maintain a register of processors.

**15 Training, confidentiality agreements and staff conduct**

15.1 The school will provide regular data protection and confidentiality training and guidance to all staff, governors and volunteers. Induction will include obligations under this policy.

15.2 Staff and volunteers handling sensitive information will sign or be notified of confidentiality expectations; breaches may lead to disciplinary action.

**16 Privacy notices and transparency**

16.1 The school publishes clear privacy notices for pupils, parents/carers, staff and governors explaining how data is used, the lawful basis for processing and the rights available. Privacy notices will be kept up to date and easily accessible.

**17 Monitoring, review and enforcement**

17.1 Compliance with this policy will be monitored by the DPO and Headteacher. The policy will be reviewed at least annually or sooner in response to legislative change, incidents or identified weaknesses.

17.2 Non-compliance may result in disciplinary action and, where appropriate, referral to regulatory authorities.

**18 Complaints and escalation**

18.1 Data protection complaints or concerns should be raised with the DPO or Headteacher in the first instance. If unresolved, complainants may contact the Information Commissioner's Office.

**19 Practical guidance and contact details**

19.1 For guidance, subject access requests or to report a breach contact:

- **Data Protection Lead / DPO:** Andy Graham
- **Headteacher:** Oz Sparks
- **School Office:** office@carltoncolvilleprimary.co.uk

19.2 For further information about rights or to complain to the regulator contact the Information Commissioner's Office at ico.org.uk..