Caradog Primary School

DATA PROTECTION POLICY

VERSION: 2.0

2026

Document Information

Version: 2.0

Status: Active

Date: 09/03/2026

Contents

1. INTRODUCTION

1.1 The School collects personal and, at times, sensitive information to carry out its functions and meet legal and regulatory obligations. It also has responsibilities to share information where required by law or in the public interest.

1.2 Regardless of how personal data is collected, recorded or used, it must be handled appropriately to ensure compliance with data protection legislation.

1.3 Lawful and responsible processing of personal data is essential to the School's operations and reflects its commitment to accountability and transparency.

1.4 This Policy outlines the School's approach to managing personal data. It applies to all staff and includes organisational measures and individual responsibilities designed to ensure compliance with data protection legislation and to uphold the rights of individuals.

2. LEGAL REQUIREMENTS

UK Data Protection Law

2.1 The UK's data protection framework is governed by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). These laws set out how personal data must be handled and the rights of individuals whose data is processed.

2.2 Personal data is defined as information relating to an identified or identifiable individual ("data subject"). The law applies to all personal data, regardless of when it was collected.

2.3 Organisations, including schools, must comply with key principles of lawful processing, including fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

2.4 Individuals have rights under UK data protection law, including the right to access their data, request rectification or erasure, object to processing, and data portability.

2.5 The Information Commissioner's Office (ICO) is the UK's independent regulator for data protection. It has a range of enforcement powers, including:

- **Public reprimands** – formal warnings issued for breaches, increasingly used for public bodies.
- **Enforcement notices** – requiring organisations to take specific actions to comply with the law.
- **Assessment notices** – allowing the ICO to carry out audits.
- **Warnings and advice** – issued where there is a risk of non-compliance.
- **Prosecutions** – for criminal offences under the DPA 2018.
- **Information notices** – requiring organisations to provide evidence or documentation.

2.6 The UK data protection regime continues to evolve. The Data (Use and Access) Act 2025 introduces reforms to enforcement and oversight, including the replacement of the ICO with a new regulator, the Information Commission, expected to take effect from December 2025.

This Policy will be reviewed and updated as further provisions of the Act are enacted and additional statutory guidance is issued.

3. SCOPE

3.1 This Policy applies to all staff employed by the School, and to external organisations or individuals who process personal data on behalf of the School.

3.2 This Policy also applies to Governors when acting in their official capacity, and to any personal data they process on behalf of the School in connection with their governance responsibilities.

3.3 The Policy covers all processing of personal data for which the School is the Data Controller. This includes:

- Personal data processed directly by the School
- Personal data controlled by the School but processed by a third party on its behalf (e.g. confidential waste disposal, or an IT supplier hosting school data in the cloud))
- Personal data processed jointly by the School and its partners

3.4 Data subjects may include, but are not limited to:

- Students/pupils
- Parents/carers or representatives
- Student/pupil contacts
- Staff and individuals working within the School, including:
  - Prospective, current and former employees (permanent, temporary, casual)
  - Student teachers
  - Work experience students
  - Volunteers
- Employee contacts
- Governors
- Suppliers and vendors
- Visitors and members of the public
- Others with whom the School communicates (e.g. facilities hirers)

3.5 The Policy applies to all personal data regardless of the format or media in which it is held, including electronic data, CCTV footage, video and sound recordings, and physical records (e.g. paper files).

4. LINKS TO OTHER POLICIES

4.1 This Policy is supported by a range of policies, procedures, guidance and documents that help staff understand and apply data protection principles in practice. These resources form part of the School's wider approach to managing information and demonstrate a commitment to accountability and transparency.

5.0 GENERAL DATA PROTECTION REGULATION - PRINCIPLES

5.1 Article 5 of the UK GDPR sets out six key principles that summarise the responsibilities placed on organisations. The School is committed to complying with each of these principles, as outlined below:

5.2 Lawfulness, Fairness and Transparency (Article 5(1)(a))

The School will process personal data in a lawful, fair and transparent way. This means:

- **Lawful basis:** The School will identify and document a lawful basis for each processing activity
- **Special category data:** Where sensitive data is processed (e.g. health, ethnicity), the School will meet additional conditions under the UK GDPR and DPA 2018.
- **Consent:** Where consent is required, the School will ensure:
    - Requests are clear, specific and easy to understand
    - Consent is actively given (no pre-ticked boxes)
    - Individuals can refuse or withdraw consent without disadvantage
    - Instructions for withdrawing consent are clear and accessible
- **Transparency:** The School will explain clearly to individuals:
    - What personal data is collected
    - Why it is needed and how it will be used
    - Who it may be shared with and why
    - How long it will be kept
    - How individuals can update their data or exercise their rights

  This information will be provided through Privacy Notices. Notices will be published on the School's website and updated when necessary. Significant changes will be communicated directly.

5.3 Purpose Limitation (Article 5(1)(b))

The School will ensure that personal data is collected for clear, specific and legitimate purposes, and not used in ways that are incompatible with those purposes.

5.4 Data Minimisation (Article 5(1)(c))

The School will only collect and retain personal data that is adequate, relevant and limited to what is necessary for its intended purpose.

5.5 Accuracy (Article 5(1)(d))

The School will:

- Keep personal data accurate and up to date where required or necessary.
- Correct inaccuracies promptly.
- Share updates internally where necessary to maintain accuracy.
- Notify relevant external partners (e.g. the Local Authority or other organisations with whom data is shared) where updates are needed to ensure their records are also accurate

5.6 Storage Limitation (Article 5(1)(e))

The School will:

- Retain personal data only for as long as necessary for the purpose it was collected.
- Apply its Retention and Disposal Guidelines to determine appropriate retention periods.
- Dispose of personal data securely (e.g. shredding, confidential waste).
- Ensure this principle is applied to both manual records (e.g. paper files) and electronic records (e.g. emails, databases, cloud systems)

5.7 Integrity and Confidentiality (Security) (Article 5(1)(f))

The School will:

- Restrict access to personal data to those who need it.
- Provide data protection training to staff and others handling personal data.
- Implement and monitor security measures as part of its wider information governance.
- Support secure working practices, including remote working.
- Ensure third parties processing data on the School's behalf sign Data Processor Agreements and meet security standards.
- Prevent international transfers unless appropriate safeguards (e.g. Standard Contractual Clauses) are in place.
- Use Information Sharing Agreements where appropriate to govern joint working.
- Ensure secure disposal of personal data in all formats when no longer needed.

6.0 INFORMATION RIGHTS

6.1 Under the UK GDPR, individuals have specific rights regarding their personal data. The School is committed to supporting these rights and has procedures in place to ensure staff can recognise and respond to requests appropriately. A summary of these rights is provided below:

i. Right to be informed

Individuals have the right to clear, accessible information about how their personal data is used. The School meets this requirement through Privacy Notices, which explain what data is collected, why it is needed, how it is used, and who it may be shared with. Notices are written in plain language and tailored to the audience (e.g. pupils, parents, staff).

ii. Right of access

Individuals can request confirmation of whether the School holds their personal data, understand how it is used, and receive a copy of that data.

The School has specific procedures in place for handling Subject Access Requests (SARs) in line with data protection legislation. Staff responsible for managing SARs, typically the Data Protection Lead, must complete relevant training provided by the Council's Information Management Team to ensure requests are handled lawfully, accurately and within statutory timeframes.

iii. Right to correct incorrect information (rectification)

If personal data is inaccurate or incomplete, individuals can request that it be corrected.

iv. Right to erasure

Also known as the "right to be forgotten", this allows individuals to request deletion of their personal data where there is no compelling reason for its continued use. This right applies in specific circumstances.

v. Right to restrict processing

Individuals can ask the School to limit how their data is used, for example if they contest its accuracy or object to its use. This right applies in certain situations and is not absolute.

vi. Right to data portability

In limited circumstances, individuals can request a copy of their personal data in a structured, commonly used electronic format to transfer to another organisation.

vii. Right to object to the use of your information

Individuals can object to the processing of their personal data:

- Where processing is based on public task or legitimate interests
- For direct marketing purposes
- For profiling or automated decision-making
- For research or statistical purposes

viii. Rights in relation to automated decision making and profiling

Individuals have the right to challenge decisions made solely by automated means (without human involvement) that significantly affect them. This includes profiling used to evaluate aspects of their behaviour or characteristics.

7. ROLES AND RESPONSIBILITIES

7.1 All staff must understand their responsibilities when handling personal data. This supports compliance with data protection legislation, establishes clear lines of accountability, and promotes a culture where personal information is respected and protected.

7.2 Specific roles and governance arrangements have been established to support compliance. These include:

i. Data Protection Officer (Statutory Post)

Under Article 37 of the UK GDPR, public authorities (including maintained schools) must appoint a Data Protection Officer (DPO). The Council's Data Protection and Improvement Manager is the designated DPO for the School.

The DPO's responsibilities include:

- Advising the School and staff on data protection obligations
- Monitoring compliance with legislation and internal policies
- Raising awareness and delivering training
- Acting as the point of contact for the Information Commissioner's Office (ICO)

ii. Schools Data Protection Working Group (SDPWG)

The SDPWG is a representative group comprising Head Teachers, School Data Protection Leads, and key Local Authority staff. It plays a central role in supporting schools to meet their data protection obligations and in delivering the services outlined in the Service Level Agreement (SLA) with RCTCBC.

Key functions or the group include:

- *Acting as a formal consultation and approval body for changes to shared tools and frameworks, including the Data Protection Registers (DPRs)*
- *Facilitating communication and coordination on data protection matters across the school community*
- *Providing feedback and input into policy development, training, and guidance materials*

iii. Information Asset Owners (IAOs)

Typically senior leaders (e.g. Head Teachers), IAOs are responsible for the proper management of information systems and assets. They ensure:

- Personal data is protected and handled appropriately
- Staff comply with the six GDPR principles (see Section 5)
- Information sharing is governed by appropriate safeguards

iv. Link Governor for Data Protection

The School has a designated Link Governor for Data Protection who acts as the liaison between the governing body and the School on data protection matters.

v. Data Protection Lead (DPL)

The School's DPL oversees day-to-day data protection compliance and acts as the main point of contact for staff. They liaise directly with the Council's DPO for advice and guidance and promote good practice across the School.

vi. All Data Users

Most staff handle personal data as part of their role. Everyone has a responsibility to manage information appropriately throughout its lifecycle, from creation to secure disposal.

Individual responsibilities include:

- Complying with this Policy (non-compliance may lead to disciplinary action)
- Completing relevant training and awareness activities
- Preventing data breaches through careful handling
- Reporting suspected breaches promptly

8. RECORDS OF PROCESSING ACTIVITY

8.1 Under the UK GDPR, organisations must document their personal data processing activities. To meet this requirement, Data Protection Registers (DPRs) are maintained by the Council's Information Management Team on behalf of the School, under a Service Level Agreement (SLA).

Each DPR records key details about processing activities, including:

- The lawful basis for processing
- Categories of personal data
- Categories of data subjects
- The location of personal data (e.g. system used or storage method)
- Information sharing arrangements (internal and external)
- Retention requirements

Schools are responsible for notifying the Council of any changes to their processing activities to ensure the DPRs remain accurate and up to date.

8.2 DPRs are reviewed regularly by the Council's Information Management Team or at the request of schools. Any changes to the structure or content of the DPRs are consulted on and approved by the Schools Data Protection Working Group to ensure they reflect operational needs and support consistency across schools.

9. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

9.1 The School applies privacy by design principles when developing or changing systems and processes that involve personal data.

9.2 Specifically, the School will:

- Carry out proportionate DPIAs to identify and reduce data protection risks, particularly when introducing new technology or where processing may pose a high risk to individuals' rights and freedoms.
- Collect, use and retain only the minimum personal data necessary for the intended purpose (data minimisation).
- Anonymise personal data where appropriate, for example when using data for statistical or reporting purposes.

10. BREACHES OF PERSONAL DATA

10.1 Under the UK GDPR, organisations must report certain types of personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, where feasible.

10.2 If a breach is likely to result in a high risk to individuals' rights and freedoms, those affected must also be informed without undue delay.

10.3 The School has procedures in place to detect, report and investigate personal data

breaches. These aim to ensure that:

- Breaches are identified, categorised and monitored consistently
- Incidents are assessed and responded to appropriately
- Steps are taken to reduce the impact of any disclosure
- Mitigation measures are implemented to prevent recurrence
- Serious breaches are reported to the ICO
- Lessons learned are shared and actions agreed to help prevent future incidents

10.4 The School will consult the Council's Data Protection Officer (DPO) for advice and guidance on breach handling, and will take appropriate action based on that advice.

11. DATA PROTECTION COMPLAINTS

11.1 The School is committed to handling any concerns or complaints about how personal data is processed in a fair, transparent and timely manner. Complaints will be managed in line with this Policy and the School's Complaints Policy.

11.2 Individuals may raise data protection concerns directly with the School's Data Protection Lead using the contact details below, or through any method outlined in the School's Complaints Policy.

FAO: Rhian Derrick
Caradog Primary School, Clifton Street, Aberdare, RCT, CF44 7PB
Email: admin@caradogprimary.rctcbc.cymru

11.3 Currently, under the UK GDPR, individuals have the right to ask the Information Commissioner's Office (ICO) to assess whether their personal data has been handled in accordance with the law. However, the Data (Use and Access) Act 2025 introduces a new statutory right to complain, which will require individuals to first raise their concerns directly with the data controller. Once this change comes into force, individuals will only be able to escalate their complaint to the ICO (or the new Information Commission) after receiving a response from the organisation.

The School will update its procedures and privacy information to reflect this change once the relevant provisions are enacted.

The Information Commissioner's Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF
www.ico.org.uk
Telephone: 0303 123 1113

11.4 The School will respond promptly and fully to any request for information or compliance assessment made by the ICO.

Appendix I

DEFINITIONS

GDPR	UK General Data Protection Regulation
DPA	Data Protection Act 2018
School	For the purposes of this document, references to 'the School' include the School's governing body acting in its official capacity.
Personal data	Any information relating to an identified or identifiable natural person ('data subject'). This includes identifiers such as name, address, date of birth, identification number, location data, online identifiers, or factors relating to physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of data	Formerly known as sensitive data, this refers to personal data that requires additional protection. Categories include: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetic data ● Biometric data (used for unique identification) ● Health data ● Data concerning a person's sex life or sexual orientation
Criminal Convictions	While not classified as special category data under the UK GDPR, personal data relating to criminal convictions and offences is subject to specific rules under Article 10 of the UK GDPR and Schedule 1 of the DPA 2018.
Data Subject	A living individual to whom personal data relates. Within the School, this may include pupils, staff, parents, volunteers.
Data Controller	The person or organisation that determines the purposes and means of processing personal data. Data Controllers are responsible for ensuring compliance with data protection law.
Data Processor	A person or organisation that processes personal data on behalf of the Data Controller and in accordance with their instructions.
Processing	Any operation performed on personal data, including (but not limited to) collecting, recording, organising, storing, using, disclosing, altering, or deleting the data.
Data User	Any member of staff, contractor or third party who processes personal data held by, or on behalf of, the School.

Information Commissioner	The Crown-appointed individual responsible for overseeing and enforcing data protection, privacy and freedom of information legislation in the UK.
ICO	Information Commissioner's Office – the UK's independent authority for data protection.

Document Control

Policy	Data Protection Policy
Owner	Caradog Primary School
Initial Policy Launch Date	09/03/2026
Review date	09/03/2026 This Policy will be reviewed every three years, or sooner if required due to changes in legislation, statutory guidance, or operational practices.

Document Approvals

This document requires approval of the governing body.

Version Control

Version No	Date Approved	Valid From Date	Valid To Date
2.0	09/03/2026	09/03/2026	09/09/2029