Carlton VC Church of England Primary School

Subject Access Request Policy 2026

'I am the vine, you are the branches; those that abide in me and I in them will bear much fruit' (John 15:5)

Approved by:	Jo Bevis Staff Governors	Date:
Written by: Notaro	Jo Bevis and Jasmine	Date: 4/1/26
Last reviewed on:		
Next review:		

Contents

1. **Purpose** .....
2. **Scope** .....
3. **Making a Subject Access Request** .....
4. **Verification of Identity** .....
    4.1 Acceptable Forms of Identification .....
    4.2 Methods of Verification .....
5. **Requests Made on Behalf of Others** .....
6. **Timeframe for Response** .....
7. **Fees** .....
8. **Exemptions and Redactions** .....
9. **Format of Response** .....
10. **Complaints** .....

1. Purpose

This policy outlines the procedure for handling Subject Access Requests (SARs) in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Individuals have the right to request access to personal data that we hold about them. We are committed to responding to requests lawfully, transparently, and within the statutory timeframes.

2. Scope

This policy applies to all Subject Access Requests received by the organisation, whether made by:

- Employees
- Parents or carers
- Pupils (where appropriate)
- Contractors
- Former employees or pupils
- Any other individual whose personal data we process

Requests may be made in writing, by email, or verbally.

3. Making a Subject Access Request

A Subject Access Request can be made in any format and does not need to include the phrase "Subject Access Request" to be valid.

Requests should be directed to:

Jo Bevis – Head Teacher jbevis@carltonvcprimary.co.uk

4. Verification of Identity

Before processing any Subject Access Request, the organisation must verify the identity of the individual making the request.

This applies:

- Even where the individual is known to us
- Even where the request is made by a current employee, parent, or pupil
- In all cases without exception

We will not begin processing a Subject Access Request until identity has been satisfactorily verified.

4.1 Acceptable Forms of Identification

We may request one or more of the following:

- Photographic identification (e.g. passport or driving licence)
- Proof of address (e.g. utility bill, bank statement dated within the last three months)

4.2 Methods of Verification

Verification may be completed by one of the following methods:

In Person Verification

- We may require the individual to attend in person to present identification.
- Original documents must be shown.

Email Submission of Identification

- We may accept scanned or photographed copies of identification sent by email.
- However, this will always be followed up by a telephone call to the individual.

Telephone Verification

- During the follow-up call, the individual may be required to answer security questions to confirm their identity.
- The organisation reserves the right to determine appropriate security questions.

The one-month statutory timeframe for responding to a SAR will begin only once identity has been verified.

If satisfactory identification is not provided, the request will not proceed.

5. Requests Made on Behalf of Others

If a request is made by a third party (e.g. solicitor, relative, parent on behalf of an adult child), we will require:

- Written authority from the data subject; and
- Verification of identity for both the requester and the data subject.

6. Timeframe for Response

We will respond to Subject Access Requests within:

- One calendar month of verifying identity.

Where a request is complex or numerous, we may extend the response time by a further two months. The individual will be informed within the first month if an extension is required.

7. Fees

Subject Access Requests are normally free of charge.

However, we may charge a reasonable administrative fee if:

- The request is manifestly unfounded or excessive; or
- Further copies of the same information are requested.

8. Exemptions and Redactions

In certain circumstances, information may be withheld where exemptions apply under data protection legislation, including but not limited to:

- Third-party personal data
- Confidential references
- Safeguarding information
- Legal privilege

Where information is redacted or withheld, the individual will be informed where appropriate.

8.1 Safeguarding and Data Protection Considerations in Subject Access Requests

The school recognises its dual responsibilities under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, alongside its statutory safeguarding duties under *Keeping Children Safe in Education (KCSIE)* and the Children Act 1989 and 2004.

While individuals have a legal right to access their personal data through a Subject Access Request (SAR), this right is not absolute. The school will always balance the right of access against its safeguarding obligations and the rights and freedoms of others.

8.2 Safeguarding Exemptions

The school reserves the right to withhold, redact, or restrict disclosure of information where providing that information would:

- Place a child, young person, staff member, or other individual at risk of harm;
- Prejudice the prevention or detection of crime;
- Prejudice an ongoing safeguarding investigation;
- Interfere with an active child protection plan, early help assessment, or social care involvement;
- Reveal information provided by third parties where consent has not been given and disclosure would be unreasonable;
- Disclose information that identifies another individual who has not consented to disclosure.

In particular, where there is:

- An open safeguarding concern;
- Ongoing involvement from Social Care, the Police, or another safeguarding agency;
- A child protection plan or strategy meeting in place;

- Advice from the Local Authority Designated Officer (LADO) or other statutory body not to disclose;

the school may delay, restrict, or refuse disclosure where permitted under the Data Protection Act 2018 exemptions.

3.2 Application of Exemptions

Any decision to withhold or redact information will be:

- Made on a case-by-case basis;
- Clearly documented, including the rationale for applying an exemption;
- Approved by the Headteacher
- Made in consultation with safeguarding leads and, where appropriate, external agencies.

Where information is withheld, the school will inform the requester that an exemption has been applied, unless doing so would itself compromise safeguarding or legal proceedings.

The welfare and safety of children is paramount. Where there is any conflict between data protection rights and safeguarding duties, the school will prioritise its safeguarding responsibilities in accordance with statutory guidance.

For further clarification and a rationale of the above, please read Appendix A

9. Format of Response

Information will normally be provided:

- Electronically (secure email) unless otherwise requested; or
- In paper format where appropriate.

10. Complaints

If an individual is dissatisfied with how their request has been handled, they may:

- Raise a complaint in line with the school's complaint policy and/or
- Lodge a complaint with the Information Commissioner's Office (ICO).

Information Commissioner's Office
Website: www.ico.org.uk
Telephone: 0303 123 1113

Carlton VC CofE Primary School

Appendix A

Rationale for Excluding Safeguarding and Child Protection Information from SAR Documents

At Carlton CofE Primary School, the handling of Subject Access Requests (SARs) is governed by the principles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, alongside statutory safeguarding obligations as outlined in *Keeping Children Safe in Education 2025*.

1. **Legal Basis Under UK GDPR and Data Protection Act 2018**
   The UK GDPR mandates that personal data must be processed fairly and lawfully, with particular attention to the rights and freedoms of data subjects (Article 5). However, it also allows for certain exemptions where disclosure would adversely affect the rights and freedoms of others. Specifically, safeguarding and child protection information often contains highly sensitive data about third parties (including other children and families), which must be protected to prevent harm or distress.
2. **Safeguarding Considerations**
   According to *Keeping Children Safe in Education 2025* (paragraph 94), safeguarding and child protection must underpin all policies and processes, ensuring the best interests of the child are paramount. The guidance emphasises that safeguarding policies should be transparent and accessible but also stresses the need for careful handling of sensitive information to protect children's welfare (paragraphs 96-98).
3. **Risk of Harm and Confidentiality**
   Disclosure of safeguarding or child protection information in a SAR may inadvertently reveal details about other children or vulnerable individuals, potentially causing significant harm, distress, or risk to those individuals. The school has a duty to maintain confidentiality and to safeguard all pupils, which includes managing information sharing responsibly.
4. **Proportionate and Risk-Based Approach**
   The school adopts a proportionate, risk-based approach to information sharing as advised by the DfE safeguarding guidance (paragraph 100). This means that when responding to SARs, information that could compromise safeguarding

arrangements or the welfare of others is withheld to prevent harm, while still complying with data protection principles.

5. **Balancing Rights and Safeguarding**
   While individuals have the right to access their personal data, this right is balanced against the need to protect children and others from harm. The school ensures that SAR responses are carefully redacted or limited to exclude safeguarding and child protection records when disclosure would not be in the best interests of the child or others involved.
6. **Procedural Safeguards and Transparency**
   The school's safeguarding policies clearly outline the handling and sharing of sensitive information and are reviewed regularly to align with legal requirements (paragraph 98). Parents and pupils are informed about the limits of data access where safeguarding concerns exist, maintaining transparency and trust.

Summary

Carlton CofE Primary School does not send safeguarding or child protection documents in response to SARs because:

- UK GDPR and the Data Protection Act 2018 allow withholding information to protect the rights and freedoms of others.
- Safeguarding guidance requires prioritising the welfare and safety of all children, preventing harm through inappropriate disclosure.
- The school employs a proportionate, risk-based approach to protect sensitive information.
- Confidentiality and safeguarding obligations outweigh the right to access certain personal data when disclosure could cause harm.

This approach ensures compliance with legal frameworks while maintaining the highest standards of child protection.