Carlton VC Church of England Primary School

Data Protection Policy 2025-2026

'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: October 2025
Written & Edited by: Jo Bevis	Date:: October 2025
Last reviewed on: May 2025	
Next review: May 2026	

Data Protection Policy

Carlton C of E Primary School is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors.

The DFE collects and uses information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents; this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. It also takes into account the provisions of the General Data Protection Regulation, which came into force in 2018. This policy complies with our funding agreement and articles of association.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

1) Introduction

i) Carlton Primary School needs to keep certain information about our employees, pupils and other users to allow us, for example, to monitor performance, achievement, and health and safety.

ii) To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, we must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 and updated in the GDPR 2018.

iii) In summary these principles state that personal data shall:

(a) Be obtained and processed fairly and lawfully.

(b) Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

(c) Be adequate, relevant and not excessive for that purpose.

(d) Be accurate and kept up to date.

(e) Not be kept for longer than is necessary for that purpose.

(f) Be processed in accordance with the data subject's rights.

(g) Be kept safe from unauthorised access, accidental loss or destruction.

iv) Personal data shall be kept secure i.e. protected by an appropriate degree of

security ;

v) Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

All staff who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

2) Responsibilities of Staff

i) All staff are responsible for:

(a) Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

(b) Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

(c) Handling all personal data (e.g. – pupil attainment data) with reference to this policy.

3) Data Security

i) All staff are responsible for ensuring that:

(a) Any personal data that they hold is kept securely.

(b) Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

ii) Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

iii) Personal information should:

(a) Be kept in a filing cabinet, drawer, or safe in a secure office, or;

(b) If it is computerised, be password protected both on a local hard drive and on a network drive that is regularly backed up; and

(c) If a copy is kept on a USB memory key or other removable storage media, that media must itself be password protected and/or kept in a filing cabinet, drawer, or safe.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be stored in a locked cupboard in the office. Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.
- USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.
All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.
All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.
Disposal of IT assets holding data shall be in compliance with ICO guidance:
https://ico.org.uk/media/fororganisations/documents/1570/it_asset_disposal_for_organisations.pdf
The school has identified a qualified source for disposal of IT assets and collections.
The school also uses Shred-it to dispose of sensitive data that is no longer required.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Carlton school address……

A charge may be applied to process the request.

4) Retention of Data

i) The School has a duty to retain some staff and pupil personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

5) **Monitoring and Evaluation**

This is ongoing; where any clarifications or actions are needed the Policy will be amended at its next review.

This is a link to the Government website with full details of the GDPR 2018.
https://www.gov.uk/data-protection