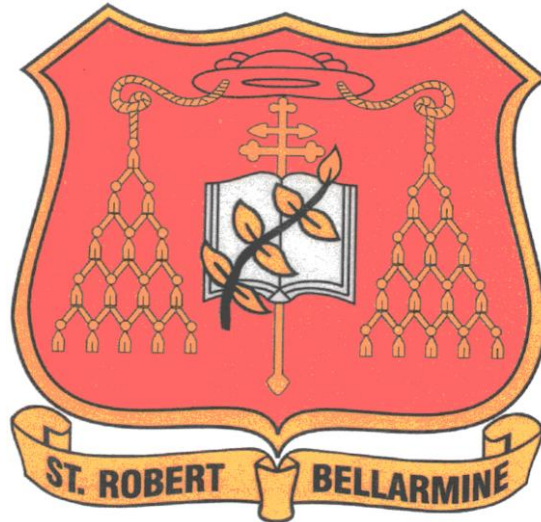


St Robert Bellarmine Catholic Primary School



Data Protection Policy

Our Mission Statement

"We are God's work of art."

Help each other

Be happy

Follow the light of Jesus

Include everybody

Everybody do their best in every way

Be friends with everyone

Be responsible for your own actions

Be Respectful

Work to the best of your abilities

Parents, teachers and children support each other.

Data Protection Policy

Contents

- 1. Aims**
- 2. Legislation and Guidance**
- 3. Definitions**
- 4. The Data Controller**
- 5. Roles and Responsibilities**
- 6. Data Protection Principles**
- 7. Collecting Personal Data**
- 8. Sharing Personal Data**
- 9. Subject Access Requests and Other Rights of Individuals**
- 10. Parental Requests to See the Educational Record**
- 11. Biometric Recognition Systems**
- 12. CCTV**
- 13. Photographs and Videos**
- 14. Data Protection by Design and Default**
- 15. Data Security and Storage of Records**
- 16. Disposal of Records**
- 17. Personal Data Breaches**
- 18. Training**
- 19. Monitoring Arrangements**
- 20. Links with Other Policies**

Appendix 1: Personal Data Breach Procedure

1. Aims

St Robert Bellarmine Catholic Primary School is required to keep and process certain personal data about its staff, pupils and other individuals in order to fulfil its statutory duties, provide education, and meet its legal obligations.

The school is committed to ensuring that all personal data is:

- collected and used lawfully, fairly and transparently;
- stored securely;
- not disclosed unlawfully;
- processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This policy applies to all personal data, whether held electronically or in paper format.

All staff receive data protection training and are expected to understand and comply with this policy. Any breach may result in disciplinary action.

2. Legislation and Guidance

This policy is based on:

- UK General Data Protection Regulation (UK GDPR)
 - Data Protection Act 2018
 - Information Commissioner's Office (ICO) guidance
 - ICO Code of Practice on Subject Access Requests
 - ICO Surveillance Camera Code of Practice
 - Education (Pupil Information) (England) Regulations 2005
-

3. Definitions

Personal data – Information relating to an identified or identifiable living individual.

Special category personal data – More sensitive data requiring additional protection, including data about health, ethnicity, religion, and biometric data.

Processing – Any operation performed on personal data.

Data subject – The individual to whom the personal data relates.

Data controller – The organisation that determines how and why personal data is processed.

Data processor – A person or organisation that processes data on behalf of the controller.

Personal data breach – A breach of security leading to accidental or unlawful loss, disclosure or access to personal data.

4. The Data Controller

St Robert Bellarmine Catholic Primary School is the Data Controller.

The school is registered with the Information Commissioner's Office (ICO).

Data Protection Lead: Mr L Dinsdale

Contact number: 0151 928 5601

5. Roles and Responsibilities

5.1 Governing Body

The Governing Body has overall responsibility for ensuring compliance with data protection legislation and that this policy is reviewed every two years.

5.2 Data Protection Officer (DPO)

The DPO oversees compliance with data protection law and acts as the point of contact with the ICO.

DPO: Mrs Jayne Austin

Email: finance.strobertbellarmine@schools.sefton.gov.uk

5.3 Headteacher

The Headteacher ensures that data protection obligations are met on a day-to-day basis and that staff receive appropriate training.

5.4 All Staff

All staff are responsible for handling personal data securely and reporting concerns or breaches immediately to the DPL or DPO.

6. Data Protection Principles

Personal data will be:

- processed lawfully, fairly and transparently;
 - collected for specified, explicit purposes;
 - adequate, relevant and limited;
 - accurate and up to date;
 - retained only as long as necessary;
 - processed securely.
-

7. Collecting Personal Data

The school processes personal data under lawful bases including public task, legal obligation, vital interests, and consent where appropriate.

Consent is not relied upon where processing is required to meet statutory duties, including safeguarding.

Privacy notices are provided to pupils, parents, staff and visitors explaining how data is used.

8. Sharing Personal Data

Personal data is only shared when lawful and necessary, including with:

- local authorities;
- safeguarding partners;
- government bodies;
- approved contractors.

All third parties are required to meet data protection standards.

9. Subject Access Requests and Other Rights

Individuals have the right to access their personal data.

Requests will be responded to within one month.

Information will be provided free of charge, unless the request is manifestly unfounded or excessive, in which case a reasonable fee may be charged or the request refused.

Children's Requests

There is no fixed age at which a child can exercise data protection rights. Competence will be assessed on a case-by-case basis.

10. Parental Requests to See the Educational Record

Parents have a legal right to free access to inspect their child's educational record within 15 school days.

A reasonable fee may be charged for copies only.

11. Biometric Recognition Systems

Reviewed Jan 2026

The school does not currently use biometric systems. Written parental consent would be required before any such system is introduced.

12. CCTV

CCTV is used for crime prevention, safeguarding and site security. We currently do not have up to date CCTV.

13. Photographs and Videos

Written parental consent is obtained before using pupil images for communication or promotional purposes.

Consent can be withdrawn at any time.

Images are not accompanied by full names or identifying information.

14. Data Protection by Design and Default

The school embeds data protection into all processing activities, including risk assessments and staff training.

15. Data Security and Storage

Appropriate technical and organisational measures protect personal data, including password controls, encryption, and secure storage.

16. Disposal of Records

Personal data is securely destroyed in line with the school's Records Retention Schedule.

17. Personal Data Breaches

All breaches are reported immediately to the DPL/DPO. Where required, breaches are reported to the ICO within 72 hours.

18. Training

All staff and governors receive data protection training as part of induction and ongoing professional development.

19. Monitoring Arrangements

The DPO monitors compliance and this policy is reviewed every two years.

20. Links with Other Policies

- Child Protection Policy
 - Freedom of Information Policy
 - E-Safety Policy
 - Records Retention Schedule
-

Appendix 1: Personal Data Breach Procedure

All suspected breaches must be reported immediately to the DPO.

Breaches are investigated, contained, recorded and, where necessary, reported to the ICO and affected individuals in line with UK GDPR requirements.

Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO by emailing data@englishmartyrs.co.uk
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPL will alert the headteacher and the chair of governors
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- The DPO & DPL will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self assessment tool. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the School's computer system.
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
 - A description of the nature of the personal data breach including, where possible:
 - The categories and approximate number of individuals concerned
 - The categories and approximate number of personal data records concerned

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
 - The name and contact details of the DPO
 - A description, in clear and plain language, of the nature of the personal data breach
 - A description of the likely consequences of the personal data breach
 - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the School's computer system.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPL as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPL will ask the ICT department to recall it

- In any cases where the recall is unsuccessful, the DPL will contact the DPO and relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked

The school's cashless payment provider was hacked and parents' financial details