

St Monica's Catholic Primary School



St Monica's Privacy Notices 2026-2028

Approved by:	Headteacher Governing Board	Date: July 2026
Next review due by:	July 2028	

Contents

1. About this notice and who we are
2. A quick explanation for pupils
3. The information we collect
4. Why we use pupil information and our lawful bases
5. Where information comes from
6. Information that is required and information that is optional
7. Who we share information with
8. Department for Education and the National Pupil Database
9. Photographs, videos, CCTV, online services and artificial intelligence
10. International transfers
11. How long we keep information
12. How we protect information
13. Pupil and parent/carer rights
14. Requests and data protection complaints
15. Contact details

[Appendix A: Summary of common processing activities](#)

1. About this notice and who we are

St Monica's Catholic Primary School is the data controller for the personal information described in this notice. This means that the school decides why and how the information is used. The school is registered with the Information Commissioner's Office (ICO).

This notice applies to pupils in the Early Years Foundation Stage and Key Stages 1 and 2. It is provided to parents and carers because they usually supply information and act on behalf of younger children. Data protection rights belong to the pupil, and the school will involve and explain matters directly to a child where this is appropriate for their age and understanding.

We aim to provide privacy information in clear language. A paper copy, large-print version, translated explanation or other reasonable support is available free of charge from the School Office.

2. A quick explanation for pupils

What this means for you

We keep information about you so that we can teach you, support you, keep you safe and run the school properly.

We only use what we need and we do not sell it. We share it only for a good and lawful reason. You can ask what we hold or tell us if something is wrong by speaking to a trusted adult, your parent or carer, the Headteacher or the Data Protection Officer.

3. The information we collect

Depending on the pupil and the services involved, the school may process the following categories of personal information:

- identification and contact information, including name, former names, date of birth, sex, address, telephone numbers, email addresses, unique pupil number and admission details;
- parental responsibility, family, emergency contact and household information;
- pupil characteristics, including ethnicity, first language, nationality or country of birth where required, religion, eligibility for free school meals and pupil premium, looked-after or previously looked-after status, service-child status and young-carer information;
- education information, including class, curriculum, learning records, assessment, attainment, phonics, multiplication tables and national curriculum results;
- attendance information, including sessions attended, absence, lateness, reasons and previous schools;
- special educational needs and disability information, including needs, provision, plans, professional advice and reasonable adjustments;
- health, medical, dietary, allergy, medication, accident, first-aid and wellbeing information;
- safeguarding and child-protection information, including concerns, referrals, court orders, professional involvement, early help and pastoral support;
- behaviour, relationships, bullying, suspension, permanent exclusion, alternative provision and reintegration information;
- school meals, trips, clubs, extended services, transport, payments, debt and eligibility information;
- photographs, video and audio recordings, pupil work, CCTV images and event information;
- digital and technical information, including usernames, school email, device and network identifiers, access logs, filtering and monitoring alerts, platform use, cyber-security events and online-safety records;
- communications, complaints, requests, consent choices and views expressed by pupils, parents or carers; and
- any other information that is necessary for a defined education, safeguarding, health, legal, operational or support purpose.

Special category information includes information about health, ethnicity, religion and other particularly sensitive matters. We apply additional legal conditions and safeguards when using it.

The school does not currently use automated biometric recognition systems and does not hold or process pupils' biometric information for identification. This is confirmed in the school's Statement of Not Holding Biometric Data.

4. Why we use pupil information and our lawful bases

We use pupil information to:

- admit pupils, maintain the school roll and manage day-to-day pupil administration;
- teach the curriculum, assess learning, monitor progress and report to pupils and families;
- support attendance, inclusion, SEND, pastoral care, health and wellbeing;
- safeguard children, prevent harm and respond to emergencies, concerns or allegations;
- manage behaviour, relationships, bullying, suspensions and permanent exclusions fairly;
- provide meals, trips, clubs, wraparound or other school services;
- communicate with families and provide information about school life;
- keep the site, people, systems and information secure;
- manage complaints, legal claims, insurance, audit and governance;
- evaluate and improve teaching, support and school services;
- meet funding, census, assessment, attendance and other statutory reporting duties; and
- use photographs, recordings or pupil work for agreed communication or promotional purposes where this is genuinely optional.

4.1 Main lawful bases

Under Article 6 of the UK GDPR, the school normally relies on one or more of the following lawful bases:

- **Legal obligation** - the processing is necessary to comply with education, safeguarding, equality, health and safety, funding, employment, financial or other legal duties.
- **Public task** - the processing is necessary for the school to perform its education and public-authority functions in the public interest.
- **Vital interests** - the processing is necessary to protect someone's life or physical safety, particularly in an emergency.

- **Consent** - used only where the activity is genuinely optional and consent can be refused or withdrawn without unfair disadvantage, for example some external publicity uses of photographs or videos.
- **Contract** - used in limited circumstances where processing is necessary for a specific agreement or service requested by a parent or carer.

4.2 Special category and criminal offence information

Where we process special category information, we also identify an Article 9 condition and any condition required by the Data Protection Act 2018. Depending on the purpose, this may include substantial public interest, safeguarding children and individuals at risk, health or social care, equality monitoring, research and statistics with safeguards, legal claims, or explicit consent where appropriate.

Criminal offence information is processed only where authorised by law and necessary for safeguarding, prevention or detection of unlawful acts, legal proceedings or another defined statutory purpose.

Relevant legislation includes the Education Acts, Children Acts, Children and Families Act 2014, Equality Act 2010, Education (Pupil Information) (England) Regulations 2005, Education (Information About Individual Pupils) (England) Regulations 2013 as amended, UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025. The exact lawful basis for each processing activity is recorded in the school's Record of Processing Activities.

5. Where information comes from

We obtain personal information from sources including:

- pupils and their parents or carers, including admissions, consent, medical, contact and update forms;
- previous schools, early years providers and the Common Transfer File or secure School to School system;
- teachers, support staff, school leaders and authorised governors;
- Sefton Council, the Department for Education and other public bodies;
- health professionals, the NHS, school nursing and immunisation services;
- children's social care, safeguarding partners, police, courts and other agencies;
- approved educational technology, management information, payment, catering and communication systems;
- CCTV, school devices, accounts, networks, filtering and monitoring systems; and
- other people or organisations where there is a lawful and proportionate reason to receive the information.

6. Information that is required and information that is optional

Most pupil information is required so that the school can fulfil its legal duties and provide education, safeguarding and support. Where information is mandatory, we will explain this at the point of collection and, where relevant, the consequences of not providing it.

Some information is optional. We will make this clear and explain the intended use. Refusing or withdrawing optional consent will not affect a pupil's core education or entitlement. However, the school may be unable to provide the specific optional activity or publish the relevant material.

Where consent is our lawful basis, it may be withdrawn at any time by contacting the School Office. Withdrawal does not make earlier lawful processing unlawful. Printed, distributed or lawfully published material may not always be capable of complete retrieval.

7. Who we share information with

We share personal information only where there is a lawful basis and the sharing is necessary, proportionate and secure. Consent is not always required, particularly where information must be shared to meet a legal duty, perform a public task, protect a child or prevent or detect crime.

Depending on the circumstances, recipients may include:

- the Department for Education and Sefton Council;
- the school or educational setting a pupil attends after leaving St Monica's, and alternative provision where used;

- health professionals, school nursing, immunisation teams, NHS services and emergency services;
- children's social care, safeguarding partners, the local authority designated officer, police, courts and Prevent partners;
- the Standards and Testing Agency and other authorised assessment bodies;
- the Archdiocese of Liverpool and diocesan education bodies where information is needed for lawful governance, admissions, school support or oversight;
- catering, transport, trip, club, photography and other service providers where necessary;
- IT, educational technology, management information, payment, communications, cyber-security and cloud-service providers acting under contract;
- insurers, auditors, legal advisers, professional advisers and regulators; and
- governors and authorised school personnel who have a legitimate need to know.

Suppliers and contractors are given only the information necessary to provide their service. We undertake proportionate due diligence and use contracts or other safeguards requiring them to protect information, follow our instructions and delete or return it when appropriate.

The school does not sell pupil or family personal information.

8. Department for Education and the National Pupil Database

The Department for Education (DfE) collects information from schools and local authorities through statutory data collections, including the school census. As a maintained school, we are required to provide information under section 537A of the Education Act 1996 and the Education (Information About Individual Pupils) (England) Regulations 2013, as amended. Consent is not required for these statutory returns.

The information supports school funding, education policy, accountability, research, statistics and the monitoring of children's education and wellbeing. Some information is stored in the National Pupil Database (NPD), which is owned and managed by the DfE. The DfE may share information from the NPD where it is lawful, secure and ethical, including with schools, local authorities, researchers, other public bodies and organisations promoting children's education or wellbeing.

Further official information:

- [DfE privacy information for learners from EYFS to Key Stage 3](#)
- [National Pupil Database privacy notice](#)
- [School data collections and censuses](#)
- [DfE external data shares](#)

9. Photographs, videos, CCTV, online services and artificial intelligence

9.1 Photographs, video and audio

The school may take photographs, video or audio for teaching, assessment, safeguarding, internal records and school activities. Where material is intended for newsletters, the website, social media, media coverage, marketing or other external promotion, the school will normally obtain written consent and explain the intended use.

Parents and carers may take photographs at some school events for personal use, subject to school instructions. They should not publish images of other children without the relevant family's agreement and must follow any safeguarding restrictions announced by the school.

9.2 CCTV

CCTV is used in identified locations to help protect pupils, staff, visitors and school property, prevent or investigate incidents and support site security. Images are accessed only by authorised people, kept for no longer than necessary and disclosed only where there is a lawful reason, such as safeguarding, crime prevention, legal proceedings or a valid rights request. Enquiries about CCTV should be directed to the Headteacher.

9.3 Online services and educational technology

The school uses approved digital platforms and educational technology to support teaching, communication, administration, safeguarding and security. These services may process account details, work, communications and technical information. The school assesses providers, configures services appropriately, limits access and updates privacy information where a new use materially affects pupils or families.

9.4 Artificial intelligence and automated decision-making

Personal data, special category data, safeguarding information and confidential information must not be entered into a generative AI tool unless the tool and the proposed use have been formally assessed and authorised. Before using personal information in an AI system, the school will identify a lawful basis, review security and provider terms, consider whether data is retained or used for training, update privacy information and complete a data protection impact assessment where required.

The school does not currently make decisions about pupils that have legal or similarly significant effects solely by automated means. Digital tools may support professional judgement, but an appropriately informed member of staff remains responsible for significant decisions. If this changes, the school will update this notice and explain the safeguards and rights that apply.

10. International transfers

Some approved suppliers may store or access information outside the United Kingdom. Where this occurs, the school will ensure that the transfer is lawful and protected by an adequacy regulation, approved contractual safeguards, another permitted transfer mechanism or a specific legal exception. Further information about relevant safeguards can be requested from the Data Protection Officer.

11. How long we keep information

We keep personal information only for as long as it is needed for the purpose for which it was collected, to meet legal and regulatory requirements, and to protect the rights and interests of pupils and the school. Retention periods are set out in the school's Records Management Policy and Retention Schedule.

- When a pupil changes school, the pupil record is normally transferred securely to the receiving school through the Common Transfer File or School to School system.
- Safeguarding and child-protection records are transferred separately, securely and in accordance with safeguarding guidance.
- Some records may be retained after a pupil leaves where required by law, audit, safeguarding, insurance or legal-claim requirements.
- CCTV, technical logs and routine operational records are retained for the shortest proportionate period unless an incident, investigation or legal hold requires longer retention.
- Information may be anonymised so that it no longer identifies an individual. Anonymised statistics may be retained for longer to monitor trends and improve services.

If a legal claim, safeguarding review, investigation or other formal hold applies, relevant records will not be destroyed until the hold is lifted.

12. How we protect information

The school uses organisational and technical safeguards appropriate to the sensitivity and risk of the information. These include:

- role-based access controls and confidentiality requirements;
- secure accounts, strong authentication and managed devices;
- encryption, secure transfer methods, backups, patching and malware protection where appropriate;
- staff training, acceptable-use rules and clear reporting routes;
- processor due diligence, contracts and supplier oversight;
- data protection by design, risk assessment and data protection impact assessments for higher-risk uses; and

- a personal data breach procedure, including assessment, containment, recording and notification to the ICO or affected individuals where required.

No system can remove every risk, but the school regularly reviews its controls and responds promptly when a weakness or incident is identified.

13. Pupil and parent/carers rights

Pupils have rights under data protection law. A parent or carer may exercise a child's rights where the child authorises them or is not sufficiently mature to act independently. The school will consider the child's age, understanding, best interests, confidentiality and any safeguarding implications.

Depending on the circumstances and lawful basis, rights may include:

- the right to be informed about how personal information is used;
- the right of access to personal information, usually through a subject access request;
- the right to ask for inaccurate or incomplete information to be corrected;
- the right to erasure in limited circumstances;
- the right to restrict processing in limited circumstances;
- the right to object to certain processing, including direct marketing;
- the right to data portability where the legal conditions apply;
- rights concerning solely automated decision-making and profiling; and
- the right to withdraw consent where consent is the lawful basis.

These rights are not absolute. For example, the school may need to retain and use information to comply with a legal obligation, perform its public task, protect a child, preserve another person's rights or maintain confidential safeguarding information.

A subject access request is normally answered within one month. School holidays do not pause the time limit. A parent of a pupil at a maintained school also has a separate right to request access to their child's educational record under the Education (Pupil Information) (England) Regulations 2005; the usual response period for that request is 15 school days. The two rights are different and information may be withheld where a legal exemption applies.

14. Requests and data protection complaints

14.1 Making a rights request

A request does not need special wording. Please describe the information or action required and provide enough detail to help us identify the relevant records. We may ask for proof of identity, parental responsibility, authority to act for a pupil or clarification of a request. We will not ask for more information than is reasonably necessary.

14.2 Raising a data protection complaint

If you believe the school has not handled personal information properly, you can make a data protection complaint verbally or in writing to the School Office, Headteacher, Data Protection Lead or Data Protection Officer. Please explain what happened, whose information is involved, the outcome you are seeking and any relevant dates or documents.

The school will help people to make a complaint, acknowledge receipt within 30 days, investigate without undue delay, keep the complainant appropriately informed and communicate the outcome without undue delay. Complaints are handled in accordance with the Data Protection Policy and the school's data protection complaints procedure.

You may also complain to the Information Commissioner's Office. It is usually helpful to give the school an opportunity to address the matter first, but this does not remove the right to contact the ICO.

15. Contact details

Contact	Details
Data controller	St Monica's Catholic Primary School Kelly Drive, Bootle, Merseyside, L20 9EB Telephone: 0151 525 1245 Email: finance.stmonicas@schools.sefton.gov.uk Website: www.stmonicascatholicprimaryschool.co.uk
Data Protection Lead	James Gouldbourne, Headteacher Email: ht.stmonicas@schools.sefton.gov.uk
Data Protection Officer	Kevin Doherty Email: governance@nexus-global.co.uk Suite 9a, Stanley Grange, Ormskirk Road, Knowsley, L34 4AT
Information Commissioner's Office	Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Helpline: 0303 123 1113 Website: ico.org.uk

To request a paper or accessible copy of this notice, contact the School Office. The most current version will be made available on the school website.

Appendix A: Summary of common processing activities

This table summarises common uses of pupil information. It is not a complete Record of Processing Activities and does not replace the fuller explanations in this notice or the Data Protection Policy.

Activity	Typical information	Main purpose	Main lawful basis
Admissions and pupil administration	Identity, address, contacts, parental responsibility, previous school, eligibility	Admit pupils, maintain roll and records, communicate with families	Legal obligation; public task
Teaching, assessment and reporting	Learning, curriculum, attainment, pupil work, assessment results	Deliver education, monitor progress and report	Public task; legal obligation
Attendance	Sessions, absence, lateness, reasons and daily attendance data	Improve attendance, safeguard pupils and make statutory returns	Legal obligation; public task
SEND and inclusion	Needs, disability, plans, adjustments, professional advice	Assess and provide suitable support and reasonable adjustments	Legal obligation; public task; Article 9 condition
Safeguarding and pastoral care	Concerns, referrals, family circumstances, professional involvement	Protect children, provide early help and coordinate support	Legal obligation; public task; vital interests; Article 9 condition
Health and welfare	Medical needs, allergies, medication, accidents, dietary needs	Keep pupils safe and provide appropriate care	Legal obligation; public task; vital interests; Article 9 condition
Behaviour and exclusions	Incidents, support, sanctions, suspensions, exclusion records	Maintain safety, fairness and lawful behaviour management	Legal obligation; public task
Meals, trips and services	Eligibility, dietary needs, payments, emergency contacts	Provide school services and activities safely	Public task; legal obligation; contract where applicable
Statutory returns and funding	Census, characteristics, attendance, attainment, funding indicators	Meet DfE and local authority duties and allocate funding	Legal obligation; public task

Activity	Typical information	Main purpose	Main lawful basis
Security, CCTV and technical logs	Images, device/network identifiers, access and security logs	Protect people, premises, systems and information	Public task; legal obligation; legitimate interests where appropriate
Communications and publicity	Photographs, video, pupil work, contact preferences	Share school news and celebrate achievement	Public task for internal use; consent for optional external promotion
Approved EdTech and AI	Accounts, work, usage data and only authorised personal information	Support learning, administration or safeguarding	Public task or legal obligation; consent only where genuinely optional

Last updated: July 2026. This notice reflects the school's current processing arrangements and will be updated when there is a material change in law, systems, suppliers or practice.