Micklehurst All Saints CE Primary School

Pupil and parent carer privacy notice

Updated September 2026 | Version 2.0 | England

This notice explains how we use personal information about pupils, parents, carers and emergency contacts, why we need it, who we share it with and the rights you have. You do not need to sign or consent to this privacy notice. Optional publicity choices are provided separately at the end.

Who is responsible for your information

The data controller, which decides how and why personal information is used, is Miss Laura Trelfa, Headteacher, Micklehurst All Saints CE primary School, The Rowans, Mossley, OL5 9DR, e-mail: admin@micklehurstallsaints.tameside.sch.uk, telephone 01457 83 2128.

Our Data Protection Officer service is provided by Global Policing Limited. Email: data@globalpolicing.co.uk. Telephone: 0161 510 2999 (answerphone). Website: www.globalpolicing.co.uk/data. You may contact the school or the DPO about this notice or your rights.

We follow the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended, including by the Data (Use and Access) Act 2025.

Information we collect and where it comes from

We collect information from you and your child, previous schools, local authorities, education and health professionals, and safeguarding agencies. We also create records during education and school activities. Information may include:

- Names, dates of birth, addresses, contact details, pupil identifiers, parental responsibility, emergency contacts and relevant family circumstances.
- Admissions, attendance and absence reasons, attainment, assessments, behaviour, exclusions, school transfers, trips and support provided.
- Special educational needs and disabilities, health and allergy information, care plans, safeguarding concerns and referrals; ethnicity, religion or other characteristics where relevant and lawful.
- Parent and carer communications, complaints, payment and funding eligibility information, including free school meal eligibility; photographs and system-use records where applicable.

Why we use information and our lawful bases

We use information to provide education, support learning and wellbeing, manage attendance and behaviour, protect children, communicate with families, administer services and funding, and meet reporting and record-keeping duties. We use the minimum information needed for each purpose.

Education and school administration

As a maintained school, delivering education and associated pastoral and administrative functions normally relies on public task under Article 6(1)(e). Compliance with a specific statutory duty relies on legal obligation under Article 6(1)(c). These bases cover necessary processing rather than an unrestricted right to use

information. Applicable education duties may include the Education Act 1996 and the Education (Information About Individual Pupils) (England) Regulations 2013, as amended, for relevant pupil information returns.

Health safeguarding and other sensitive information

Health, ethnicity, religion and certain other information require an additional condition under Article 9. For necessary safeguarding we may use substantial public interest under Article 9(2)(g), with the applicable Data Protection Act 2018 Schedule 1 condition, including paragraph 18 for safeguarding children and individuals at risk where its requirements are met. Other statutory functions may use paragraph 6 where applicable, eg when we handle SEND data (creating Educational Health Care Plans), we process sensitive health and disability data in line with Article 9 and Schedule 1 provision. We maintain an appropriate policy document where required.

Criminal offence information is handled only where Article 10 and the applicable domestic-law authorisation permit it.

In a genuine emergency we may rely on vital interests under Article 6(1)(d). For special category information, Article 9(2)(c) also requires that the person is physically or legally incapable of consenting. Routine health support is not automatically treated as an emergency.

Optional uses and required information

We seek freely given, specific consent under Article 6(1)(a) for optional publicity uses where appropriate. Essential education, necessary safeguarding, lawful school transfers and statutory returns do not depend on signing the optional form. We identify our lawful basis before using information.

When requesting information we explain whether it is required by law, needed to provide a service or optional, and the consequences of not providing it. Missing essential details may prevent us from arranging a requested service or suitable support. Please tell the school when your details change.

Sharing protecting and retaining information

We share relevant information only where necessary and lawful. Depending on the purpose, recipients include receiving schools and colleges, our local authority, Tameside Metropolitan Borough Council and its commissioned services, the Department for Education (DfE), examination bodies, health professionals, safeguarding partners, social care, police or courts, and providers supporting school services.

School suppliers may support management information, learning platforms, IT, communications, payments and trips. When acting as our processors, they must follow our documented instructions and contractual security obligations; individual parental permission is not automatically required for their necessary work. Other recipients may be independent controllers with their own privacy notices.

We share statutory pupil information with the DfE where the relevant duties apply. The DfE is responsible for its own processing and explains its uses and further sharing at https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter. This includes information about the National Pupil Database, census, assessment and attendance data.

Security and school technology

Access is limited to people who need information for their work. We use appropriate organisational and technical safeguards and verify identity and authority before releasing personal information. Medical care information is shared only with those who need it; optional publicity consent does not authorise unrestricted display of medical details. We utilise several layers of technology to maintain security, ensure safety, and comply with legal safeguarding obligations.

CCTV
What is captured: Visual video recording of students, staff and visitors within specific areas of the school grounds
Why: to maintain site security, deter crime and protect the personal safety of the school community.
Lawful Basis: Legal Obligation (UK GDPR Article 6(1)(f)) and Public Task (Article 6(1)(e)) balanced against individuals privacy expectations
Who can access it: Access of recordings is restricted to the senior leadership team.
Retention: Footage is automatically overwritten on a rolling cycle, typically 30 days unless required for an ongoing investigation, see CCTV Policy.

Online Filtering and Monitoring Systems
What is Captured: Web browsing histories, search queries, accessed URLs, and keywords typed on school devices or while connected to the school network.
Why: To protect children from illegal, inappropriate, or harmful material online, fulfilling the statutory obligations outlined in Keeping Children Safe in Education (KCSIE).
Lawful Basis: Legal Obligation (UK GDPR Article 6(1)(c)) and Public Task (Article 6(1)(e)).
Who Can Access It: Automated systems flag high-risk activity directly to the Designated Safeguarding Lead (DSL) and the IT Administration team.
Retention: System logs are typically retained for 12 months or the duration of the academic year, unless an entry becomes part of a broader, active safeguarding record.

Separate Notice: Detailed operational parameters are found in the school's Online Safety Policy

Biometric Systems: are not currently used in school.

Artificial Intelligence (AI) Uses
Status in School Technology: AI technologies like **Live Facial Recognition (LFR)** or AI-driven behavioural prediction are **not used** on school grounds.
Why: Regulatory bodies like the Information Commissioner's Office (ICO) state that live facial recognition poses disproportionately high risks to pupil privacy and is highly unlikely to meet the strict legal thresholds required for educational environments. AI integration is strictly limited to standard, non-intrusive algorithmic categorization found in baseline filtering software.

How long we keep information

We apply different retention periods to different records. Our retention schedule is available at Retention Periods

It sets out the periods or criteria for pupil and parent records, safeguarding, attendance, finance, images and system logs. We consider legal duties, safeguarding needs, transfers and the time reasonably needed to

handle complaints or legal claims. Records subject to a lawful preservation requirement are retained until it ends.

Primary pupil records normally transfer to the next school; secondary pupil records are generally retained to the pupil's 25th birthday. Safeguarding records may need longer retention, including child sexual abuse records under current guidance. There is no blanket promise to erase all information at age 25 or all parent information when a child leaves. We securely destroy or anonymise records when no longer needed.

Your rights and how to contact us

You can ask for access to your personal information and correction of inaccurate or incomplete information. Depending on the lawful basis and circumstances, you may also ask for erasure, restriction of use or a portable copy, or object to processing. These rights have conditions and exceptions; for example, we may need to retain records to meet a legal duty.

Where we rely on consent, you can withdraw it at any time without affecting the lawfulness of earlier use. Where we rely on public task or legitimate interests, you may object on grounds relating to your circumstances. You can object to direct marketing at any time.

Contact the school or our DPO to exercise your rights. Requests can be made verbally or in writing and do not have to use a particular form. We may need proportionate evidence of identity or authority to protect your information. We normally respond to a subject access request within one calendar month. Where the law allows clarification, an extension or an exemption, we will explain how this affects your request. School holidays do not automatically extend the deadline.

Personal information rights belong to the child as well as to parents in relation to their own information. A parent may act for a child where the child is not competent to act for themselves, or with the competent child's authority. We consider the child's understanding, wishes and interests before disclosing their information.

A parent's separate right to request an educational record depends on the school type and applicable education regulations. Where this statutory right applies, the response period is 15 school days. This is different from a UK GDPR subject access request.

Questions and complaints

If you are concerned about our use of personal information, contact the school or Global Policing Limited using the details on the first page. Our data protection complaints procedure is within our Data Protection Policy. We will acknowledge a data protection complaint within 30 days, investigate appropriately, keep you informed and provide an outcome without undue delay.

You also have the right to complain to the Information Commissioner's Office (ICO). Visit https://ico.org.uk/make-a-complaint/ or call 0303 123 1113. The ICO normally expects you to give the organisation an opportunity to address your concern first.

Keeping this notice up to date

We review this notice regularly and when our use of information changes. We will bring material changes to your attention. Next scheduled review: September 2027, or sooner if needed. Ask the school for an accessible format or help understanding this notice.