



Data Privacy Notice

We at St. Michael's V.A. Junior School and Clover Hill V.A. Infant & Nursery (All Angels' Federation) are the Data Controller for the purposes of the Data Protection Act. We collect information from you, and may receive information about you from your previous school and the Learning Records Service¹.

How we use pupil information

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Attendance information (such as sessions attended, number of absences and absence reasons);
- Behaviour/Learning Assessment information and education records;
- Special Educational Needs information;
- Learning Platforms;
- Financial Services;
- Behavioural information (such as, achievements, exclusions, internal exclusions and detentions);
- Health and Safety (including medical information such as dietary requirement and medication details);
- Safeguarding and Child Protection reports and disclosures;
- Photographs, video clips and CCTV;
- Communication and Publicity

Why we collect and use this information

We use the pupil data:

- to support pupil learning;
- to monitor and report on pupil progress;
- to provide appropriate pastoral care;

- to assess the quality of our services;
- to comply with the law regarding data sharing.

The lawful basis on which we use this information

- We collect and use pupil information under a task performed in the public interest where it relates to a child's educational progression;
- Some photographs and videos are used only after gaining explicit consent;
- Where medical data is being processed, this is processed under a legal obligation (Children and Families Act 2014 which includes a duty on schools to support children with medical conditions);
- Safeguarding data is processed under the legal obligation of The Education Act 2002. Sections 21 and 175 detail how governing bodies of schools must promote the wellbeing of pupils and take a view to the safeguarding of children at the school.
- Children and Families Act 2014 includes a duty on schools to support children with medical conditions;
- The Equality Act 2010 (England, Scotland and Wales) requires you to make reasonable adjustments to ensure that children and young people with a disability are not put at a substantial disadvantage compared with their peers;
- The Education Act 2002, Sections 21 and 175 detail how governing bodies of schools must promote the wellbeing of pupils and take a view to the safeguarding of children at the school;
- Section 3 of the Children Act 1989 places a duty on a person with the care of a child to do all that is reasonable in the circumstances for the purposes of safeguarding the child;
- Education Act 1996, relating to attendance at school.

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We collect and use pupil information under the lawful bases for processing as set out in **Article 6 of the GDPR**. At least one of these must apply whenever processing personal data:

- (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

A lawful basis for your processing under Article 6 is still required in exactly the same way as for any other personal data. The difference is satisfying the lawful basis as a specific condition under Article 9. This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

See the definitions section of this Guide for full details.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

What are the conditions for processing special category data?

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- (e) processing relates to personal data which are manifestly made public by the data subject;
- (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Collecting pupil information

Whilst most of the pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

A primary school does not need to keep copies of any records in the pupil's record, unless there is an ongoing legal action when the pupil leaves the school (unless moved outside the U.K. in which case stored for 25 years).

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us;
- our local authority;
- the Department for Education (DfE).

We routinely share relevant pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- third party processors (see list below)
 - Pupil Asset (School's Management Information System)
 - Teachers2parents (Texting Communication Provider)
 - ParentPay (Parent Payment Services)
 - Microsoft 365 (Pupil login details and internal school records)
 - Apple (Passwords for St. Michael's Account)
 - JCComtech (IT Support Services)
 - Arrow (Reading Intervention Tool)
 - Thrive (Social and Emotional Intervention Tool)
 - Maths Whizz (Maths Teaching Aid)
 - Micro-Librarian (Library Services)
 - MyBook blog (Reading Intervention)
 - Creative Corner (Schools' Website Provider)
 - NFER (Pupil Assessment and Analysis Tool)
 - Edu-key (Intervention Tracker)
 - RWI portal/Oxford Owl (Phonics Tracker)
 - The Alarm Company (Security Services)
 - Tapestry (Early Years' Home/School Learning Logs)
 - Evolve (Educational Visits and Risk Assessments)
 - Norse (School Maintenance and Meals)
 - Van Cols Photographers (Individual and Class Photographs)
 - Espresso (IT Learning Platform)
 - NCA Tools (Statutory School Assessments)
 - CEPP (Educational Psychology Services)
 - UEA (Teacher Training)
 - NHS (National Health Service)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Photography and Videos

Photographs and videos will only be collected and stored with a documented lawful basis.

Photographs and videos will be used where they are deemed essential for performing the public task of the school or relative to providing education. Where photographs are required for other purposes, these purposes will be documented and explicit consent will be sought.

The retention period for photographs and videos will be documented in the retention policy. At the end of the retention period photographs will either be destroyed or they may be retained as photos for archiving purposes in the public interest.

CCTV

CCTV may be used for the purpose of protecting the safety of staff, students and visitors and to help secure the physical premises. Notices of recording including details of the Data Controller and where a copy of this policy can be obtained will be included on clearly visible signs posted at all entrances to the school site(s).

All CCTV footage is securely stored and can only be accessed by appropriate members of staff. All images recorded by CCTV will be deleted as defined in the retention schedule.

Where The Organisation installs new CCTV cameras, a data privacy impact assessment will be carried out prior to installation.

The nominated person responsible for CCTV in The Organisation is **the school's Data Controller**.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis;
- producing statistics;
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested and;
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

<https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information to, (and for which project), please visit the following website:

<https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information that we hold about you. To make a request for your personal information, contact the data protection officer whose contact details are at the top of this notice.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed and;
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

ⁱ The Learning Records Service fits within the heart of the learner experience and is designed to support learners at all levels to access, manage and use their own achievement information - such as qualifications, awards or training received as they progress through education, training and lifelong learning.

The Learning Records Service, part of Information Management (IM) Services, provides shared services across the education sector. The Learning Records Service is built on the principle of collect once, use many times and used by all that are entitled to do so. It supports the whole of the education sector.