



Leamington Federation

Lighthorne Heath Primary School

Privacy Notice for Pupils and Parents - How we use your information

Who are we?

Lighthorne Heath Primary School, part of the Leamington Federation, is the data controller for the personal information described in this notice. This means that the school decides why and how this information is used. The school is registered with the Information Commissioner's Office (ICO), registration number Z737279X.

You can contact the school at: Lighthorne Heath Primary School, Stratford Road, Lighthorne Heath, Leamington Spa, Warwickshire, CV33 9TW; email admin2064@welearn365.com.

Our Data Protection Officer

Our Data Protection Officer (DPO) is the School Data Protection Officer Service, Warwickshire Legal Services. You can contact the DPO at schooldpo@warwickshire.gov.uk, telephone 01926 412859, or by post at Warwickshire Legal Services, Warwickshire County Council, Shire Hall, Market Square, Warwick, CV34 4RL. Please state that your enquiry relates to Lighthorne Heath Primary School.

About this privacy notice

This notice explains how we collect, use, store and share personal information about pupils and their parents/carers. It is provided in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025. We also follow current Department for Education (DfE) data protection guidance for schools and relevant ICO guidance.

We review privacy information at least annually and whenever there is a significant change to the way personal information is used. Where a new use would not reasonably be expected, we will update this notice and bring the change to the attention of affected individuals before the new processing begins.

What personal information do we collect?

- pupil identity and contact information, including name, date of birth, address, unique pupil number and emergency contacts;
- parent/carer contact information and relationship to the pupil;
- characteristics and equality information, including ethnicity, language, nationality, free school meal eligibility and other information required for statutory returns;
- admissions, attendance and absence information, including reasons for absence and relevant evidence;
- curriculum, assessment, attainment, progress and educational records, including work and teacher observations;
- SEND information, EHCPs, IEPs/individual plans, reasonable adjustments and records of specialist support;
- health, medical, allergy, dietary and medication information needed to keep pupils safe and support attendance and participation;
- safeguarding, child protection, early help, looked-after/previously looked-after status and relevant social care information;
- behaviour, bullying, suspensions/exclusions and records of restrictive interventions where applicable;
- pastoral, wellbeing, counselling and therapeutic-support information where relevant;
- photographs, video or audio recordings where we have an appropriate lawful basis, including consent where required;
- information about participation in trips, clubs, wraparound care, meals and wider school activities;
- digital identifiers, school account information and logs created when pupils use school systems, devices or networks; and

- online-safety, web-filtering and monitoring information generated by the school's safeguarding and cyber-security systems.

Where does the information come from?

Information may come from pupils and parents/carers, previous or receiving schools, Warwickshire County Council, the Department for Education, health professionals, social care, safeguarding partners, police where appropriate, commissioned specialists and services, and the school's own teaching, pastoral, safeguarding and digital systems.

Why do we use pupil and parent information?

- provide education, assess learning and monitor progress;
- identify and meet SEND, language, medical, pastoral and wellbeing needs and make reasonable adjustments;
- safeguard pupils, provide early help and meet child-protection responsibilities;
- manage attendance, admissions, behaviour and the safe operation of the school;
- provide meals, trips, clubs, wraparound care and other school services;
- communicate effectively with parents/carers and respond to enquiries and complaints;
- carry out statutory data collections and provide information to DfE and the local authority;
- protect school networks, devices and users through proportionate filtering, monitoring and cyber-security controls;
- evaluate and improve teaching, provision, inclusion and school services; and
- meet legal, regulatory, safeguarding, public-health and accountability requirements.

Our lawful bases for using personal information

We only use personal information where data protection law allows us to do so. Depending on the purpose, our lawful bases under Article 6 UK GDPR may include:

- Article 6(1)(c) - compliance with legal obligations applying to schools, including education, attendance, safeguarding and statutory data-collection duties;
- Article 6(1)(e) - performance of the school's public task in providing education, support, safeguarding and school services;
- Article 6(1)(d) - protection of vital interests in emergencies; and
- Article 6(1)(a) - consent, but only for specific activities where consent is the appropriate lawful basis and can be withdrawn.

Where we use special category data, such as health, ethnicity, religious belief, trade union membership or information about a person's sex life or sexual orientation, we also identify a condition under Article 9 UK GDPR and Schedule 1 of the Data Protection Act 2018. These commonly include employment and social protection obligations, substantial public interest, health or social care, vital interests, legal claims, or explicit consent where consent is genuinely appropriate.

Criminal offence and safeguarding-vetting information is handled only where authorised by law, including Article 10 UK GDPR and the Data Protection Act 2018, and is subject to additional safeguards and restricted access.

Filtering and monitoring

To help safeguard pupils and protect school systems, the school uses appropriate filtering and monitoring arrangements on school networks, accounts and devices. These systems may record websites or services accessed, search terms, alerts, device or account identifiers and other technical information. Authorised staff review information only where necessary for safeguarding, online safety, cyber security, acceptable-use compliance or investigation of a specific concern. The school keeps these arrangements under review and balances safeguarding needs with pupils' privacy rights.

Who may we share information with?

- Warwickshire County Council and other local authorities where relevant;
- Department for Education (DfE), including through statutory school census and attendance collections;
- schools or education settings a pupil attends after leaving us, through secure transfer of appropriate educational and safeguarding records;
- health services, school nursing, NHS services and commissioned therapists or specialists where needed;
- children's social care, safeguarding partners, police and other agencies where sharing is necessary and lawful to protect a child or another person;
- exam, assessment and education-support bodies where relevant;

- providers of school information systems, educational technology, safeguarding/filtering systems, communications, catering, trips or other services acting under contract; and
- Ofsted, auditors, courts, insurers or regulators where disclosure is legally required or necessary.

Information shared with the Department for Education

The DfE collects personal information from schools and local authorities through statutory data collections. This information is used for purposes such as funding, policy development, school accountability, statistics and research. Some pupil information is held in the National Pupil Database. DfE publishes its own privacy information explaining how it uses and shares education data. The school will provide any information required by law and will not disclose additional information without a lawful basis.

How we keep information secure

We use appropriate technical and organisational measures to protect personal information against accidental or unlawful loss, alteration, disclosure or access. Access is limited to people who need the information for their role. Our service providers must process information only on our instructions, keep it secure and meet data protection requirements.

How long we keep information

We keep different records for different periods according to their purpose and legal requirements. Core pupil educational records are normally retained and transferred securely to the next school where required. Safeguarding records follow safeguarding retention and transfer rules. Other records, such as attendance, medical administration, trips, photographs and digital logs, are retained for the periods set out in the school's retention schedule and are reviewed regularly.

Records are securely deleted, destroyed or anonymised when they are no longer required. Our retention arrangements are reviewed regularly and are informed by the school's retention schedule, DfE guidance and the Information and Records Management Society (IRMS) Schools Toolkit where applicable.

International transfers

Some suppliers may store or access information outside the UK. Where this happens, we ensure that a lawful transfer mechanism and appropriate safeguards are in place, for example UK adequacy regulations or approved contractual safeguards, and we assess the protection available for the information concerned.

Automated decision-making and artificial intelligence

We do not currently use solely automated decision-making that produces legal or similarly significant effects on pupils or parents/carers. If this changes, or if we introduce an AI-enabled system that uses personal information in a way that could materially affect individuals, we will assess the data protection risks, update our privacy information where necessary and provide meaningful information about the use of the system.

Your data protection rights

Children have data protection rights in their own right, as do adults. Depending on the circumstances and the lawful basis being used, you may have the right to:

- ask for access to your personal information and receive a copy of it;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information in certain circumstances;
- ask us to restrict the use of information in certain circumstances;
- object to particular uses of personal information in certain circumstances;
- receive personal information in a portable format where the right to data portability applies;
- withdraw consent at any time where we rely on consent; withdrawal does not affect processing already carried out lawfully; and
- challenge a decision based solely on automated processing where the law gives that right.

These rights are not absolute and may be limited where another legal duty or exemption applies. We will explain this if it affects a request. Requests can be made to the school or the DPO. We normally respond to valid data protection rights requests within one month, subject to the rules in data protection law.

Concerns and complaints

If you have a concern about how we use personal information, please contact the school or our DPO first so that we can try to resolve it. You also have the right to complain to the Information Commissioner's Office (ICO). Current contact details and complaint routes are available at ico.org.uk.

Helping pupils understand their privacy

We recognise that children have the same core data protection rights as adults. We explain privacy in age-appropriate ways through our online-safety and wider curriculum, and we can provide or explain this notice in a child-friendly format where needed.

Reviewed: September 2026

Next review: September 2027

Chair of Governors: Richard Butler