Latymer All Saints
C of E Primary School

DATA PROTECTION and FREEDOM OF INFORMATION POLICY (with Privacy notices)

Approved by the Governors -

Date of Review – January 2027

1.0 Introduction

1.1 Latymer All Saints School (the School) is a data controller for the purposes of the UK GDPR.

1.2 The School aims to ensure that all personal data collected about staff, students, parents, trustees (directors), governors, volunteers and visitors and other individuals is collected, stored, and processed in accordance with the UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Act.

1.3 The School collects and uses certain types of personal information in order to provide education and associated functions. The School may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education, and safeguarding.

1.4 This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2.0 Legislation and Guidance

2.1 This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice on Subject Access Requests.

2.2 It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

2.3 It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3.0 Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity. Note that even if names and other identifying details are removed, the data will still be personal data if, by reference to something else, the person can be identified e.g. removing all names and details, but leaving the pupil number.
Term	Definition

Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4.0 The Data Controller

4.1 The School processes data relating to parents, pupils / students, staff, governors, visitors, suppliers and others as the data controller.

4.2 The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5.0 Roles and Responsibilities

5.1 This policy applies to all staff employed by the School, and to external organisations or individuals working on our behalf.

5.2 Staff who do not comply with this policy may face disciplinary action.

5.3 The School Governors

5.3.1 The School Governors has overall responsibility for ensuring that the School and its schools comply with all relevant data protection obligations

5.4 Data Protection Officer

5.4.1 The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

5.4.2 They will provide an annual report of their activities directly to the Governors and, where relevant, report to the Board their advice and recommendations on school data protection issues.

5.4.3 The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

5.4.4 The School's DPO is Steve Durbin from Ex Cathedra Solutions Ltd. The School utilises this service through a SLA on an annual basis. The contact is as follows: Schools.Data.Protection.Officer@enfield.gov.uk

5.5 **CEO / Principal / Head teacher**

5.5.1 The Head teacher will act as the representative of the data controller on a day-to-day basis.

5.6 **All Staff**

5.6.1 Staff are responsible for:

- collecting, storing, and processing any personal data in accordance with this policy.
- informing the School of any changes to their personal data, such as a change of address.
- contacting the DPO in the following circumstances:
- with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - if they have any concerns that this policy is not being followed.
    - whenever they are engaging in a new activity that may affect the privacy rights of individuals.
    - if they need help with any contracts or sharing personal data with third parties.
    - if they need to rely on or capture consent/permissions.
    - if there has been a data breach.
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way.
    - if they need to draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK.

6.0 Data Protection Principles

6.1 The UK GDPR includes data protection principles that the School must comply with. The principles say (in abbreviated form) that personal data must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed;
- accurate and, where necessary, kept up to date;
- kept for no longer than is necessary for the purposes for which it is processed;
- processed in a way that ensures it is appropriately secure.

6.2 This policy sets out how the School aims to comply with these principles.

7.0 Collecting Personal Data

7.1 Lawfulness, fairness, and transparency

7.1.1 We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- the data needs to be processed so that the School can **fulfil a contract** with the individual, or the individual has asked the School to take specific steps before entering a contract;
- the data needs to be processed so that the School can **comply with a legal obligation;**
- the data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life; or emergency situation;
- the data needs to be processed so that the School, as a public authority, can perform a task in the **public interest**, and carry out its official functions;
- the data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden);
- the individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent.**

7.1.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

7.1.3 Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation, and accuracy

7.2.1 We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

7.2.2 If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent/permissions where necessary.

7.2.3 Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

7.2.4 This will be done in accordance with the School Retentions Policy.

7.3 Sharing personal data

7.3.1 We will not normally share personal data with anyone else, but may do so where:

- there is an issue with a student or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we may need to seek consent as necessary before doing this.
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies,

educational and operational software providers. When doing this, we will:

- only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
- establish a data sharing agreement with the supplier or contractor, either in the contract or as a stand-alone; agreement, to ensure the fair and lawful processing of any personal data we share.
- only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

7.3.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- the prevention or detection of crime and/or fraud;
- the apprehension or prosecution of offenders;
- the assessment or collection of tax owed to HMRC;
- in connection with legal proceedings;
- where the disclosure is required to satisfy our safeguarding obligations;
- research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

7.3.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

7.3.4 Where we transfer personal data to a country or territory outside the UK, we will do so in accordance with data protection law.

8.0 Subject Access Requests and Other Rights of Individuals

8.1 Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the School holds about them. This includes:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

8.2 Subject access requests must be submitted in writing, either by letter or email to the DPO.

8.2.1 They should include:

- name of individual.
- correspondence address.
- contact number and email address.
- details of the information requested.

8.3 If staff identify a subject access request, they must immediately report it to their Head teacher for action. The DPO should be consulted in all except straightforward cases.

8.4 **Children and subject access requests**

8.4.1 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

8.4.2 Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of students who are under the age of 12 may be granted without the express permission of the pupil / student.

8.4.3 By contrast, children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from parents or carers of pupils / students who are 12 and over may not be granted without the express permission of the student.

8.4.4 A student's ability to understand their rights in respect of the above will always be judged on a case-by-case basis

8.5 **Responding to subject access requests**

8.5.1 When responding to requests, we:

- may ask the individual to provide 2 forms of identification.
- may contact the individual via phone to confirm the request was made.
- will respond without delay and within 1 month of receipt of the request.
- will provide the information free of charge.
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

8.5.2 We will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual.
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- is contained in adoption or parental order records.
- is given to a court in proceedings concerning the child.

8.5.3 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

8.5.4 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

8.5 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.6 Other data protection rights of the individual in addition to the right to make a subject access request (see above), and to receive information

when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- withdraw their consent to processing at any time;
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified based on public interest;
- request a copy of agreements under which their personal data is transferred outside of the UK;
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- prevent processing that is likely to cause damage or distress;
- be notified of a data breach in certain circumstances;
- make a complaint to the ICO;
- ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

8.7 Individuals should submit any request to exercise these rights to the DPO.

8.8 If staff receive such a request, they must immediately forward it to their Head teacher and the DPO.

9.0 Biometric Recognition Systems

9.1 In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18. Where we use students' biometric data as part of an automated biometric recognition system (for example, students use fingerprints to receive school dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012.

9.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it.

9.3 The School will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

9.4 Parents/carers and students have the right to choose not to use the School's biometric system(s).

9.5 We will provide alternative means of accessing the relevant services for those pupils / students. For example, students can receive a pin number to pay for transactions at the till.

9.6 Parents/carers and pupils / students can object to participation in the School's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

9.7 As required by law, if a pupil / student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's / student's parent(s)/carer(s).

9.8 Where staff members or other adults use the School's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and

other adults can also withdraw consent at any time, and the School will delete any relevant data already captured.

10.0 CCTV

10.1 We use CCTV in various locations to ensure it remains safe.

10.2 We will adhere to the ICO's code of practice for the use of CCTV.

10.3 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded.

10.4 Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

10.5 We maintain a separate CCTV policy which is available from our school office.

11.0 Photographs and videos

11.1 As part of our regular activities, we may take photographs and record images of individuals within the School.

11.2 We will obtain written consent from parents/carers, or pupils / students aged 13 and over, for photographs and videos to be taken of students for communication, marketing, and promotional materials.

11.3 We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil / student. Uses may include:

- within schools on notice boards and in school magazines, brochures, newsletters, etc.
- outside of school by external agencies such as the School appointed photographers, newspapers, campaigns.
- on-line on the School websites or social media pages Consent can be refused or withdrawn at any time.

11.4 When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

11.5 If consent is withdrawn, we will delete the photograph or video and not distribute it further.

12.0 Data protection by design and default

12.1 We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- completing privacy impact assessments where the School's processing of personal data presents a substantial risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).

- integrating data protection into internal documents including this policy, any related policies and privacy notices.
- regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance.
- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of the School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
    - for all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

13.0 Data security and storage of records

13.1 We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. In particular:

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- papers containing confidential personal data must not be left on office and classroom desks, on staff room tables, pinned to notice/display boards, or left anywhere else where there is general access.
- complex passwords must be used to access the School computers, laptops, and other electronic devices. A password can be classed as complex when it is at least 8 characters long, contains letters and numbers and at least one special character. Staff and students will be prompted to change their passwords at regular intervals.
- encryption software is used to protect portable devices and removable media, such as laptops and USB devices as per the School Security Policy.
- Staff, pupils / students, or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see the School Security Policy for more information).

13.2 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and protected (see section 8).

14.0 Disposal of records

14.1 Personal data that is no longer needed will be disposed of securely.

14.2 Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records, and overwrite or delete electronic files.

14.3 We may also use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14.4 See the School Retentions Policy for more information on our retention periods.

15.0 Personal Data Breaches

15.1 The School will make all reasonable endeavours to ensure that there are no personal data breaches.

15.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an educational context may include, but are not limited to:

- a non-anonymised data set being lost or published accidentally.
- safeguarding information being made available to an unauthorised person.
- the theft of a school laptop containing non-encrypted personal data about students.

16.0 Training

16.1 All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

17.0 Links with other Policies

17.1 This data protection policy is part of the School Information Governance Framework.

18.0 Policy Review

18.1 This policy will be reviewed and updated every 2 years.

Appendix 1: School Personal Data Breach Notification Procedure

1.0 Scope

1.1 This procedure applies in the event of a personal data breach under Article 33 of the UK GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

1.2 All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) of the School are required to be aware of, and to follow this procedure in the event of a personal data breach.

1.3 All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the DPO immediately after becoming aware.

2.0 Breach

2.1. With any breach, the Data Protection Officer (DPO) will investigate the report and determine whether a breach has occurred.

2.2 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

2.3 The DPO will document each breach, irrespective of whether it is reported to the ICO.

2.4 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)

3.0 Procedure where the School is acting as a Data Controller

3.1 The DPO will work out whether the breach must be reported to the Information Commissioner's Office (ICO). This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:

- loss of control over their data
- discrimination
- identity theft or fraud
- pecuniary loss
- unauthorised reversal of pseudonymisation (for example, key-coding)
- damage to reputation
- loss of confidentiality
- any other significant economic or social disadvantage to the individual(s) concerned

3.2 If a risk to data subject(s) is likely, the School will report the personal data breach to the Information Commissioner's Office (ICO) without undue delay, and not later than 72 hours.

3.3 If the data breach notification to the supervisory authority has not been made within 72 hours, the DPO will submit it electronically with a justification for the delay.

3.4 If it is not possible to provide all of the necessary information at the same time the School will provide the information in phases without undue further delay.

3.5 The following information needs to be provided to the supervisory authority:

- a description of the nature of the breach.
- the categories of personal data affected.
- approximate number of data subjects affected.
- approximate number of personal data records affected.
- name and contact details of the DPO.
- known consequences, likely consequences and potential future consequences of the breach.
- any measures taken to address the breach.
- any further information relating to the data breach.

3.6 The DPO will notify the ICO. In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.

4.0 Procedure where the School is acting as a Data Processor

4.1 The School must report any personal data breach or security incident to the data controller without undue delay. These contact details must be reported to the DPO who will record the breach in the Internal Breach Register. The School will then provide the controller with all of the details of the breach. The breach notification is made by phone call and a confirmation of receipt of this information must be made by email.

5.0 Procedure for notification of a breach to the data subject(s)

5.1 If the personal data breach is likely to result in substantial risk to the rights and freedoms of the data subject, The School will notify the data subjects affected immediately and without undue delay.

5.2 The notification to the data subject describes the breach in clear and plain language, in addition to information specified in clause 4 above.

5.3 The School will take whatever measures it can to render the personal data unusable to any person who is not authorised to access.

5.4 If the breach affects a high volume of data subjects and personal data records, the School will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder the School's ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure may be used to inform those affected in an equally effective manner.

5.5 If the School has not notified the data subject(s), and the ICO considers the likelihood of a data breach will result in high risk, the School will then seek to communicate the data breach to the data subject accordingly.

6.0 Appendices - Privacy Notices

- School Privacy Notice – Parents/ Carers
- School Privacy Notice – Workforce
- School Privacy Notice – Pupils
- School Privacy Notice – Applicants
- School Privacy Notice – Governors/ Volunteers

SCHOOL PRIVACY NOTICE – PARENTS/CARERS

Privacy Notice (How we use Parent/Carer information)

Under data protection law, individuals have a right to be informed about how the School use any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store, and use personal data about parents and carers.

The categories of parent/carer information that we may collect, use, hold and share include but not restricted to:

Personal information (such as name, address, telephone number and email address).

Details in respect of pupil premium entitlements and free school meal eligibility, including National Insurance Number & date of birth.

Why we collect and use this information

We use parent/carer data:

- To enable routine and emergency contact
- To ensure admission eligibility
- To access grant funding to support student outcomes

The lawful basis on which we use this information

We collect and use parent/carer information under the following:

UK General Data Protection Regulation Article 6

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

UK General Data Protection Regulation Article 9

- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

Collecting Parent/Carer Information

Whilst the majority of parent/carer information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK 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 Parent/Carer data

We hold parent/carer data until the child leaves the school. We may also keep data beyond your child's attendance at one of our schools if this is necessary in order to comply with our legal obligations.

Who we share parent/carer information with

We routinely share parent/carer information with:

The Local Authority

Parent communications providers

Parent payment providers

Department for Education (DFE)

Central and Local Government

Health authorities

Professional advisors and consultants

Police forces, courts, and tribunals

Why we share Parent/Carer information

We share parent/carer data for the reasons noted above.

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

Requesting access to your personal data

Under data protection legislation, parents/carers the right to request access to information about them that we hold. To make a request for your personal information contact the School Business Leader at your school or the Chief Financial and Operations Officer at the School.

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 request that you raise your concern with us in the first instance. You

Contact

If you would like to discuss anything in this privacy notice, please contact: The School Data Protection Officer at: Schools.Data.Protection.Officer@enfield.gov.uk

SCHOOL PRIVACY NOTICE – SCHOOL WORKFORCE

Privacy Notice (School Workforce Information)

Under data protection law, individuals have a right to be informed about how the School and its schools use any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store, and use personal data about the School's and the schools within the School workforce.

The categories of school workforce information that we collect, process, hold and share include:

- personal information (such as name, address, date of birth, phone number of employee or teacher number, emergency contacts and proof of identification)
- special categories of data including characteristics information such as gender, age, ethnic group, and Trade Union membership.
- pre-employment checks (such as DBS checks, barred list checks (where appropriate) references, health checks and prohibition from teaching checks)
- contract information (such as start dates, hours worked, post, roles, and salary information)
- work absence information (such as number of absences and reasons) and health reports
- Payroll and pension information (such as bank details and National Insurance numbers)
- qualifications (and, where relevant, subjects taught)

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- provide statutory school workforce census returns to the Department for Education
  (DfE)
- to ensure all employees have the right to work in the UK
- ensure that we meet the statutory requirements of safer recruitment practices in line with the Keeping Children Safe in Education Statutory Guidance
- inform the development of recruitment and retention policies
- enable individuals to be paid and to pay Trade Union subscriptions on behalf of employees

The lawful basis on which we process this information

We process this information under the following:

UK General Data Protection Regulation Article 6

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- Processing is necessary for compliance with a legal obligation to which the controller is subject.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

UK General Data Protection Regulation Article 9

- 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 domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

- Processing is necessary for reasons of substantial public interest, on the basis of domestic 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 this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for a period of 6 years following the end of employment, except where other legal obligations require us to retain it for longer periods.

Who we share this information with

We routinely share this information with:

- The Department for Education (DfE)
- The School Payroll Providers
- The Local Government Pension Scheme (LGPS)
- The Teachers' Pension Scheme (TPS)
- Provider of the School Management Information System
- The School Occupational Health Provider
- The Office for National Statistics

Why we share school workforce information

We share information for the purposes noted above.

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

Department for Education (DfE)

We share workforce data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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 securely store and handle the data

To be granted access to school workforce information, organisations must comply with its 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

To contact the department: https://www.gov.uk/contact-dfe you will need to have:

- your full name
- contact telephone number (or email address if you do not have a telephone number)

Requesting Access to Your Personal Data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, please contact the School Business Leader at your establishment.

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 /

Further information

If you would like to discuss anything in this privacy notice, please contact:

The School Data Protection Officer at:

Schools.Data.Protection.Officer@enfield.gov.uk

SCHOOL PRIVACY NOTICE – PUPILS

Privacy Notice (How we use pupil information)

Under data protection law, individuals have a right to be informed about how the School and its schools uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store, and use personal data about pupils.

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

- Personal information (such as name, unique pupil number and address and telephone number)
- Characteristics (such as ethnicity, language, nationality, and country of birth
- Health information and details of specific dietary requirements
- Details in respect of pupil premium entitlements and free school meal eligibility
- Data in respect of academic attainment and progress
- Safeguarding information
- Special Educational Needs Information (SEN)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Details in respect of Exclusions
- Photos and CCTV images

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities, and the Department for Education.

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 ensure compliance with statutory health and safety legislation
- to ensure compliance with statutory safeguarding legislation
- to assess the quality of our services
- to access online educational resources
- to comply with the law regarding data sharing
- to fulfil statutory data returns to both the DfE and Local Authority

The lawful basis on which we use this information

We collect and use pupil information under the following:
UK General Data Protection Regulation Article 6

- Processing is necessary for compliance with a legal obligation
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

UK General Data Protection Regulations Article 9

- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting Pupil Information

Whilst the majority of 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

We hold pupil data until the child leaves the school. We may also keep it beyond their attendance at our schools of this is necessary to comply with our legal obligations.

Who we share pupil information with:

- Schools that the pupil attends after leaving us
- The Local Authority
- The Department for Education (DfE)
- School Management Information System provider
- School catering contractor

- School photographer
- Online educational resource providers
- Online performance data tracker provider
- Services provided by the Primary Care School, (PCT) i.e., Speech & Language, School Nurse etc.

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. We are required to share information about our pupils with the (DfE) under regulation 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

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.

National Pupil Database

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-supporti ng-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, (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, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information or be given access to your child's educational record please contact the school.

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 request 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/

Contact

If you would like to discuss anything in this privacy notice, please contact:

The School Data Protection Officer at:

Schools.Data.Protection.Officer@enfield.gov.uk

SCHOOL PRIVACY NOTICE - APPLICANTS

Privacy Notice (Job Applicants)

Under data protection law, individuals have a right to be informed about how our School uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store, and use personal data about individuals applying for jobs within our School.

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

- Name and address
- Email address and telephone number
- Date of birth
- Equal opportunities monitoring information
- Nationality and entitlement to work in the UK
- National insurance number
- Information about current salary and benefits
- Qualifications and skills

- Work experience, employment history, training records and professional memberships
- References
- Information in respect of criminal records
- Disability status to enable the School/School to make any reasonable adjustments throughout the recruitment process

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

Why we collect and use this information

The School and its schools' processes data relating to applicants in order to:

- Enable management of the recruitment process
- Facilitate safer recruitment by ensuring compliance with legal obligations
- Ensure compliance with legal obligations in relation to the right to work in the UK
- Ensure a candidate's suitability and establish relevant experience and qualifications
- Enter into an employment contract with successful appointees
- Enable ethnicity and disability monitoring
- Ensure reasonable adjustments can be made for those applicants who have a disability
- Ensure that the recruitment process is fair and non-discriminatory

The lawful basis on which we process this information

You will be asked for your consent for the School/School to hold, process and share your personal data in relation to the recruitment process.

You are under no obligation to provide your consent However, if you do not consent to the School/School holding, processing, and sharing your personal data during the recruitment process, the School/School may not be able to process your application.

In some cases, the School/School will need to process data to ensure that it is complying with its legal obligations. For example, the School/School must check an applicant's entitlement to work in the UK. Safer recruitment procedures in schools also require appropriate checks to be made on people who work with children. Where this is the case, the following legal basis will apply:

UK General Data Protection Regulation Article 6

- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract.

- Processing is necessary for compliance with a legal obligation to which the controller is subject.

UK General Data Protection Regulation Article 9

- 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 as far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

- 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.

Collecting this information

We collect this information in a variety of ways. For example:

- Application forms

- Passport or other identity documents

- Forms completed as part of the recruitment process.

- Correspondence

- Interviews, meetings, or other assessments as part of the recruitment process.

In accordance with the School/School's safer recruitment obligations, the School/School will also collect personal information about you from third parties. This will include obtaining references from your previous employer and from third parties such as the Disclosure and Barring Service (DBS) to ensure the relevant safeguarding checks are completed.

Storing this information

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

If you are successful in being appointed, all personal data collected by the school will be processed and transferred to your personnel file.

If you are unsuccessful in your application, the school will retain your personal information for a period of six months after the end of the recruitment process.

Who we share this information with

Your personal data may be shared internally with other members of staff involved in the recruitment process in order for them to perform their roles. This can include members of the School senior leadership teams, governors and our HR provider.

We may also share your personal data with third parties. This can include when obtaining background checks as part of safer recruitment guidelines, pre-employment references and criminal records checks from the DBS.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, please contact the School Business Lead at the individual school or Chief Financial and Operation Officer at the School.

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

Further information

If you would like to discuss anything in this privacy notice, please contact:
The School Data Protection Officer at:

Schools.Data.Protection.Officer@enfield.gov.uk

School Governors and Volunteers Privacy Notice

Privacy Notice (Governors/Volunteers)

Under data protection law, individuals have a right to be informed about how the School and the schools, use any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store, and use personal data about the School's Governors and Volunteers.

The categories of Governor/Volunteer information that we collect, process, hold and share include:

- personal information (such as name, address, date of birth, phone number, email, emergency contacts and proof of address and identification)
- special categories of data, including characteristics information such as nationality, gender, age, and ethnicity
- References
- Employment Details

- qualifications and professional experience
- Disclosure & Barring Service Check
- Information about business and pecuniary interests

Why we collect and use this information

We use Governors/Volunteer data to:

Fulfil statutory requirements set out in the DfE Guidance 'Keeping Children Safe in Education' in respect of safeguarding and ensuring that prospective Governors and Volunteers are not prohibited from such roles.

The lawful basis on which we process this information:

We process this information under the following:

UK GDPR Article 6

- Processing is necessary for compliance with a legal obligation to which the controller is subject.

UK GDPR Article 9

- Processing is necessary for reasons of substantial public interest, on the basis of domestic 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 this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Information Held

We maintain a file to store personal information about all volunteers. The information contained in this file is kept secure and is only used for purposes directly relevant to your work with the School.

When your relationship with the School has ended, we will retain and dispose of your personal information in accordance with our Data retention schedule.

Storing this information

We hold Volunteer and Governor data in accordance with out retention policy.

Who we share this information with

We routinely share this information with:

- The Department for Education (DfE)
- Companies House
- The Disclosure and Barring Service
- Our accountants and auditors
- The National Governors Association
- Governor Hub
- The Clerking provider to the School

Sharing information.

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

Department for Education (DfE)

We share Governor/Volunteer data with the Department for Education (DfE) on a statutory basis.

Data collection requirements

In line with the requirements of the School Funding agreement there is a statutory requirement to provide details in respect of Local Governing Board Members to the Secretary of State via the secure Edubase System. The information provided will be publicly available.

To contact the department: 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 about you that we hold. To make a request for your personal information, please contact the School.

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

Further information

If you would like to discuss anything in this privacy notice, please contact:

The School Data Protection Officer at:

Schools.Data.Protection.Officer@enfield.gov.uk