St Olave's Grammar School

DATA PROTECTION GDPR POLICY

This policy has been revised in light of the European Union's General Data Protection Regulation, hereafter GDPR (May 2018), the advice for school leaders issued by the DfE in December 2017 related to GDPR, the Children Act 1989, and the Education Acts of 1996 and 2005.

Introduction

As a school, St Olave's collects and processes personal data for its pupils under the auspices of Section 537A of the Education Act 1996 and Section 83 of the Children Act 1989; it collects personal data for staff under Section 114 of the Education Act 2005. Processing of personal data is necessary to comply with the legal obligations of the designated Data Controller (see below).

Aims and Objectives

St. Olave's Grammar School takes seriously its responsibility for accountability regarding Data Protection. The aims of this policy are to ensure the school's compliance with GDPR and to affirm its accountability to the following principles:

- The school will process personal data lawfully, fairly and in a transparent manner;
- The school will collect personal data for specified, explicit and legitimate purposes;
- The school will collect personal data which is adequate, relevant and limited to what is necessary;
- The school will collect and record personal data accurately and, where necessary, keep it up-to-date;
- The school will retain personal data for the period which it deems necessary as stated in the Privacy Notices, deleting personal data when it is no longer relevant;
- The school will process personal data in an appropriate manner to maintain security.

Definitions

Personal Data for the purposes of GDPR and of this policy is defined as any information relating to an identified or identifiable natural person. Personal data means any information relating to any living individual (also known as a 'data subject') who can be identified (directly or indirectly) in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). Relevant individuals can include your colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal or business related.

Personal data may be automated (e.g. electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g. structured paper files and archives).

Processing for the purposes of GDPR and of this policy is defined as anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. It also includes sending or transferring personal data to third parties.

Data subject for the purposes of GDPR and of this policy is defined as the identified or identifiable individual whose personal data is held or processed.

Responsibilities

Data Controller: The Data Controller for St Olave's Grammar School is the Head Teacher. He, together with the Governing Body, determines the purposes and means of the processing of personal data at St Olave's Grammar school; is responsible for implementing technical and organisational measures; implements Data Protection Policies; and maintains a record of all processing activities including but not limited to: contact details, purpose, type of data, and restrictions on data retention. The Data Controller shall ensure the active involvement of the DPO (see below), and provide them with any necessary resources. The Data Controller shall be accountable to the DPO and shall facilitate the exercise of data subject rights [in accordance with Article 12, clause 2 of GDPR].

Data Processors: All people who process data on behalf of the Data Controller.

Virtually all employees of St Olave's Grammar School, whether teaching or non-teaching staff, are **Internal Processors** with a common responsibility to protect all personal data handled in the course of their duties, albeit some have specific additional responsibilities for collection and storage of particular categories of data.

In this respect, this policy applies to all staff employed by our school, and staff who do not comply with this policy may face disciplinary action.

All parties not employed by the school but with whom the school shares personal data for legitimate operational reasons are **External Processors**. The School Business Manager will ensure that contracts are in place with all such parties which specify how they will adhere and be accountable to the same six core principles of Data Protection listed above. Decisions on whether St Olave's releases data to third parties are subject to a strict approval process by the School Business Manager 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
- 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.

Data Protection Officer (hereafter DPO): The DPO will ensure the School's compliance with GDPR principles, holding it accountable to its policy and the policy's legal basis. They will have direct access as necessary to the Data Controller, Senior Leadership Team and Governing Body of St Olave's Grammar School, and will be accessible to all data subjects of St Olave's Grammar School. The DPO will: inform and advise the Data Controller on all GDPR compliance issues; monitor GDPR compliance; provide advice with regard to Data Protection Impact Assessments; and cooperate and liaise, as necessary, with the supervising authority (the ICO). St Olave's Grammar School has a reciprocal arrangement in terms of DPO with its sister school, St Saviour's, via the St Olave's and St Saviour's Foundation, with the Business Manager of each school acting as DPO to the other.

Training

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 or policies make it necessary.

Data Protection Obligations

St Olave's School is responsible for and must be able to demonstrate compliance with data protection law. To ensure that St Olave's School meets its responsibilities, it is essential that its staff and stakeholders comply with data protection law and any other St Olave's School policies, guidelines or instructions relating to personal data when processing personal data in the course of their employment.

We have set out below the key obligations under data protection law and details of how St Olave's School expects staff and stakeholders to comply with these requirements.

Legal grounds for processing
Data protection law allows us to process personal data only where there are fair and legal grounds which justify using the information.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

- complying with a legal obligation (e.g. safeguarding, health and safety or tax laws);
- entering into or performing a contract with the individual (e.g. an Employee's terms and conditions of employment);
- acting in St Olave's or a third party's legitimate interests (e.g. maintaining records of business activities, monitoring business productivity); and
- obtaining the consent of the individual (e.g. for sending direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed and unambiguous, and St Olave's School must effectively demonstrate that consent has been given.

In line with ICO guidance regarding the employer/employee relationship, St Olave's School does **not** use consent as a legal ground for processing data unless the data processing activities concerned are genuinely optional.

Transparency
Data protection law also requires us to process personal data in a transparent manner by providing individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. Appendix 1 of this policy is the 'Privacy Notice for Staff' and Appendix 2 is the 'Privacy Notice for Pupils and Parents', which explain how the school uses personal data for these categories of data subjects.

Processing personal data

Data protection law requires us to ensure that St Olave's School will only process personal data in accordance with our legitimate purposes to carry out our business operations and to administer employment and other business relationships (also known as 'data minimisation'). In other words, we ask for the information we need for our legitimate operational purposes, but we won't ask for more information than we need.

The majority of personal data which the school collects is 'ordinary', and done so by dint of legal obligation, including:

- For pupils on roll:
    - Name
    - Date of birth
    - Address
    - FSM status
    - SEND status
    - Allergies
    - Timetables
    - Subject choices
    - Attendance
    - Punctuality
- For parents/carers of pupils on roll:
    - Name
    - Contact information
    - Address
    - Relationship to pupil
- For staff:
    - Names
    - Addresses
    - Contact information
    - Salary
    - Contracts
    - Next of kin
    - Timetables
    - Qualifications
    - DBS Checks

Some categories of personal data are 'special' because they are particularly sensitive. Where special category personal data is concerned, data protection law requires us to have an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances.

If a secondary legal ground cannot be justified, St Olave's will neither collect nor process data conforming to one of the following categories without the explicit consent of the data subject:

- Race
- Ethnicity
- Political opinions
- Religion
- Philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- physical or mental Health data
- Sexual orientation
- criminal offences or convictions
- Photographs which might be used for publicity purposes

When the school seeks to collect data relating to one of these special categories, with the data subject's consent, it will only do so on the basis that "processing is necessary for reasons of substantial public interest … which is proportionate to the aim pursued and which contains appropriate safeguards" GDPR Article 9(2)(g). The consent given must be freely given, specific, informed, unambiguous, explicitly sought and retrospectively verifiable. All data subjects giving consent for the processing of these categories of personal data may withdraw said consent at any point freely and of their own volition.

In terms of pupil data, the legal age for giving consent for processing is 13. Prior to this point, parental consent must be sought. The school will retain evidence of all consent given.

All consent given prior to implementation of GDPR (May 2018) has been reviewed to ensure compliance.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible. Any enquiries about the CCTV system should be directed to the School Business Manager.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of their child for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and the pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on noticeboards and in school magazines, brochures, newsletters etc
- Outside of school such as the school photographer, newspapers, campaigns etc
- Online on our school website and/or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, we will not accompany them with personal information which clearly identifies the child.

Data Retention

Records containing personal data should only be kept for as long as they are needed for the identified purposes. The Information and Records Management Society (IRMS) is a professional association for those who work in records or information management. It has produced an information management toolkit for schools. A table on pages 37-56 shows the retention periods for different types of school records, and the actions to take at the end of a record's administrative life. St Olave's School uses this guidance when

considering data retention, storage and deletion and internal processes/guidelines regarding various types of company records and information that contain personal data.

For the IRMS Toolkit for Schools, visit
https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

We take appropriate steps to retain personal data only for so long as is necessary, taking into account the following criteria:

- the amount, nature, and sensitivity of the personal data;
- the risk of harm from unauthorised use or disclosure;
- the purposes for which we process the personal data and how long we need the particular data to achieve these purposes;
- how long the personal data is likely to remain accurate and up-to-date;
- for how long the personal data might be relevant to possible future legal claims; and
- any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

Sharing or disclosing personal data

Internal data sharing

St Olave's School ensures that personal data is only shared internally, and 'special' data on a 'need to know' basis.

As a school there are various operations that we consider part of all staff's regular activity that will involve processing ordinary information on data subjects. To mitigate against the need to continually update data mapping, we consider all St Olave's staff to potentially process ordinary data in the following means:

- SIMS
- Email
- Finance packages
- Mark books/Planners

External data sharing

We will only share personal data with other third parties (including group entities) where we have a legitimate purpose, and an appropriate legal ground under data protection law which permits us to do so. Commonly, this could include situations where we are legally obliged to provide the information (e.g. to HMRC for tax purposes or DfE Census returns) or where necessary to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers).

We may appoint third party service providers (known as processors) who will handle information on our behalf, for example to provide payroll, data storage or other technology services.

St Olave's School remains responsible for ensuring that its processors comply with data protection law and this Policy in their handling of personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor. The extent of these measures will vary depending on the nature of the activities and contractual obligations.

Details of the recipients or categories of recipients of personal data (including processors and other third parties) should be set out in privacy notices as described in Appendix 1 and 2.

The transfer of personal data to another country

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed, accessed or otherwise processed in, a different country. European Union data protection law restricts, in particular, personal data transfers to countries outside of the European Economic Area (EEA – this is the European Union plus Norway, Liechtenstein and Iceland), to ensure that the level of data protection afforded to individuals is not compromised (as the laws of such countries may not provide the same level of protection for personal data as within the EEA).

To ensure that data protection is not compromised when personal data is transferred to another country, St Olave's School assesses the risks of any transfer of personal data outside of the UK (taking into account the principles in this Policy, as well as the restrictions on transfers outside the EEA) and puts in place additional appropriate safeguards where required.

Subject Access Requests and Other Rights of Data Subjects

Data subjects have a right to make a Subject Access Request (SAR) 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
- The source of the data, if not the individual

Subject access requests must be submitted in writing, either by letter or email to the DPO. They should include:

- Name of the individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a SAR they must immediately forward it to the controller.

Children and SARs: Personal data about a child belongs to that child, and not to the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent. Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at St Olave's may not be granted without the express permission of the pupil. A pupils' ability to understand their rights will always be judged on a case-by-case basis.

Responding to SARs: When responding to SARs, we:

- May ask the individual to provide two forms of identification
- May contact the individual by phone to confirm that it was they who had made the request
- Will respond without delay and within one month of receipt of the request

- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request where a request is complex or numerous. We will inform the individual of this within one month and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil 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 court order records
- Is given to a court in proceedings concerning the child

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

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

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

Parental requests to see the educational record: Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Other rights of data subjects: Under Article 7 of GDPR, data subjects also have;

- **The right to request that we correct incomplete or inaccurate** personal data that we hold about them.
- **The right to withdraw any consent** which they have given.
- **The right to request that we delete or remove** personal data that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below).
- **The right to object to our processing** of their personal data for direct marketing purposes, or where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing.
- **The right to request that we restrict our processing** of their personal data. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
- **The right to request that we transfer** to them or another party, in a structured format, their personal data which they have provided to us (also known as the right to 'data portability'). The applicability of this right depends on the legal grounds on which we process it.
- **The right to challenge a decision** based solely on profiling/automated processing, to obtain human intervention, and to express their point of view.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one month timeframe.

Individuals also have rights to complain to the ICO about, and to take action in court to enforce their rights and seek compensation for damage suffered from, any breaches.

Data security and storage of records

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, that contain personal data, are kept password protected and securely stored when not in use
- Papers containing confidential personal data must not be left on office and classroom desks or anywhere where there is the potential for general access
- Personal passwords are required for staff and pupils to access school computers and network resources; users are obliged to change these passwords regularly (every 60 days), and passwords must be alphanumeric and at least six characters long; passwords cannot be re-used until five cycles of changed passwords have elapsed (300 days).
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see AUP).
- Where there is a 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 adequately protected.

It is considered part of the Staff Code of Conduct that data information is protected and kept within the confines of the requirements for school operation. If data is removed from the school site, it will be done so only for the purposes of fulfilling St Olave's statutory obligations in the provider of education. It will be kept secured in one of the following ways:

- Personal data used only on St Olave's own equipment and NOT on staff's personal devices. These school devices will be password protected.
- USB and memory hard drives will be encrypted
- Paper documents will be stored, transported and handled securely, with no identifying data visible to non St Olave's staff.

Data Breach Protocols and Recording of Breaches

Breaches of personal data are defined for the purposes of this policy as a breach of the security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes and such breaches might include: access by an unauthorised third party; the sending of personal data to an incorrect recipient; electronic devices containing personal data being lost or stolen; and the alteration of personal data without permission.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to individuals' personal data, St Olave's School will take immediate steps to identify, assess and address it, including containing the risks, remedying the breach, and notifying appropriate parties (see below).

If St Olave's School discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, we will report it to the ICO within 72 hours of discovery.

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the ICO.

If you become aware of any breach (or suspected breach) of this Policy you must report it to the Controller (Headteacher) to ensure that the breach is effectively assessed and addressed, and that we comply with St Olave's data breach reporting obligations. The Controller will record and report a description of the breach which includes the categories of data, the numbers of data subjects affected, the likely consequences of the breach, the measures taken to mitigate the breach and the details of the DPO. Effects and remedial actions taken will be added to the record of the breach as soon as possible to enable assessment of compliance by the DPO and/or the ICO.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken. The Controller will inform the data subject(s) concerned in plain language and without undue delay and this notification will be added to the record of the breach.

Other related policies:

Agreed User Policy (AUP), Child Protection Policy

APPENDIX 1

PRIVACY NOTICE FOR STAFF

This section of the policy explains how the School uses school workforce information for both teaching and non-teaching staff who are employed by the School. This notice will be made available to all those employed to teach or otherwise engaged to work at St Olave's in order to explain why and how their personal data is collected and processed.

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

- personal information (such as name, employee or teacher number, national insurance number, address, telephone number, personal email addresses, relevant medical information);
- special categories of data including characteristics information such as gender, age, ethnic group;
- contract information (such as start dates, hours worked, post, roles and salary information);
- work absence information (such as number of absences and reasons);
- 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
- inform the development of recruitment and retention policies
- enable individuals to be paid

The lawful basis on which we process this information

We process this information under the Education Act 2005 Section 114 (the mandatory requirement to collect staff data on the basis that a school may be required to supply prescribed information to the Secretary of State or others for a variety of qualifying purposes) and hence GDPR Article 6 [1(c)] (processing is necessary for compliance with a legal obligation); special category data is processed by the school under GDPR Article 9 [2(g)] (processing is necessary for reasons of substantial public interest).

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it (the "special category" data) 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 until the data subject is of retirement age, or until ten years has elapsed after they have left the employment of St Olave's Grammar School – whichever period of time is the longer.

Who we share this information with

We routinely share aspects of this information with:

- Our Local Authority (Bromley)
- The Department for Education (DfE)
- The St Olave's and St Saviour's Foundation
- The Rochester Diocesan Board of Education (RDBE)

Why we share school workforce information

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

Local Authority:

As a maintained school, we are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal 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 educational attainment.

St Olave's and St Saviour's Foundation and RDBE

We share personal data with these two bodies under GDPR Article 6 [1(e)] (processing is necessary for the performance of a task carried out …in the exercise of official authority vested in the controller)

Data Collection Requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) 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

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, contact the School Business Manager.

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 Business Manager

APPENDIX 2

PRIVACY NOTICE FOR STUDENTS AND PARENTS

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

- Personal information (such as name, unique pupil number [UPN] and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal [FSM] eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information
- Special Educational Needs and Disabilities [SEND] information
- Behavioural information, including that relating to exclusions
- Leavers' Destinations

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 the Education Act 1996 [537[a]) and the Children Act 1989 [83] (which dictate that we as a school are obliged to process pupil data for the purpose of Departmental Censuses) and under GDPR Article 6 [1(c)] (processing is necessary for compliance with a legal obligation); special category data is processed by the school under GDPR Article 9 [2(g)] (processing is necessary for reasons of substantial public interest).

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it (the "special category" data) 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 indefinitely.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupils attend after leaving us

- our Local Authority
- the Department for Education (DfE)
- Accredited Healthcare and Social Services providers (such as the NHS, CAMHS, MASH, the School Nurse service and Bromley Wellbeing)

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.

As a maintained school, 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 have a legal obligation and duty of care to ensure the safety, health and wellbeing of the pupils on our school roll and we therefore share personal data with accredited healthcare and social services providers as necessary under GDPR Article 6 [1(e)] (processing is necessary for the performance of a task carried out …in the exercise of official authority vested in the controller)

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.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority's website.

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. 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
- 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, contact the School Business Manager.

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 Business Manager