Brentside High School

Data Protection Policy

Ratified by Governors

<table>
<thead>
<tr>
<th>Review date</th>
<th>October 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLT responsible</td>
<td>SBM (NBA)</td>
</tr>
</tbody>
</table>
Contents

<table>
<thead>
<tr>
<th>Aims</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation and guidance</td>
<td></td>
</tr>
<tr>
<td>Definitions</td>
<td></td>
</tr>
<tr>
<td>The data controller</td>
<td></td>
</tr>
<tr>
<td>Roles and responsibilities</td>
<td></td>
</tr>
<tr>
<td>Data protection principles</td>
<td></td>
</tr>
<tr>
<td>Collecting personal data</td>
<td></td>
</tr>
<tr>
<td>Sharing personal data</td>
<td></td>
</tr>
<tr>
<td>Subject access requests and other rights of individuals</td>
<td></td>
</tr>
<tr>
<td>Parental requests to see the educational record</td>
<td></td>
</tr>
<tr>
<td>CCTV</td>
<td></td>
</tr>
<tr>
<td>Photographs and videos</td>
<td></td>
</tr>
<tr>
<td>Data protection by design and default</td>
<td></td>
</tr>
<tr>
<td>Data security and storage of records</td>
<td></td>
</tr>
<tr>
<td>Disposal of records</td>
<td></td>
</tr>
<tr>
<td>Personal data breaches</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
</tr>
<tr>
<td>Monitoring arrangements</td>
<td></td>
</tr>
<tr>
<td>Links with other policies</td>
<td></td>
</tr>
<tr>
<td>Appendix 1: Personal data breach procedure</td>
<td></td>
</tr>
<tr>
<td>Appendix 2: Privacy Notice for Brentside High School</td>
<td></td>
</tr>
</tbody>
</table>
Aims
Brentside High School aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

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

Legislation and Guidance
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner’s Office (ICO) and the ICO’s code of practice for subject access requests.

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

In addition, this policy complies with regulation 5 of the Education (Student Information) (England) Regulations 2005, which gives parents the right of access to their student’s educational record.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified, or identifiable, individual.</td>
</tr>
<tr>
<td></td>
<td>This may include the individual’s:</td>
</tr>
<tr>
<td></td>
<td>• Name (including initials)</td>
</tr>
<tr>
<td></td>
<td>• Identification number</td>
</tr>
<tr>
<td></td>
<td>• Location data</td>
</tr>
<tr>
<td></td>
<td>• Online identifier, such as a username</td>
</tr>
<tr>
<td></td>
<td>It may also include factors specific to the individual’s physical,</td>
</tr>
<tr>
<td></td>
<td>physiological, genetic, mental, economic, cultural or social identity.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>Personal data which is more sensitive and so needs more protection,</td>
</tr>
<tr>
<td></td>
<td>including information about an individual’s:</td>
</tr>
<tr>
<td></td>
<td>• Racial or ethnic origin</td>
</tr>
<tr>
<td></td>
<td>• Political opinions</td>
</tr>
<tr>
<td></td>
<td>• Religious or philosophical beliefs</td>
</tr>
<tr>
<td></td>
<td>• Trade union membership</td>
</tr>
<tr>
<td></td>
<td>• Genetics</td>
</tr>
<tr>
<td></td>
<td>• Biometrics (such as fingerprints, retina and iris patterns), where used</td>
</tr>
<tr>
<td></td>
<td>for identification purposes</td>
</tr>
<tr>
<td></td>
<td>• Health – physical or mental</td>
</tr>
<tr>
<td></td>
<td>• Sex life or sexual orientation</td>
</tr>
<tr>
<td>Processing</td>
<td>Anything done to personal data, such as collecting, recording, organising,</td>
</tr>
<tr>
<td></td>
<td>structuring, storing, adapting, altering, retrieving, using, disseminating,</td>
</tr>
<tr>
<td></td>
<td>erasing or destroying.</td>
</tr>
<tr>
<td></td>
<td>Processing can be automated or manual.</td>
</tr>
<tr>
<td>Data subject</td>
<td>The identified or identifiable individual whose personal data is held or</td>
</tr>
<tr>
<td></td>
<td>processed.</td>
</tr>
<tr>
<td>Data controller</td>
<td>A person or organisation that determines the purposes and the means of</td>
</tr>
<tr>
<td></td>
<td>processing of personal data.</td>
</tr>
<tr>
<td>Data processor</td>
<td>A person or other body, other than an employee of the data controller,</td>
</tr>
<tr>
<td></td>
<td>who processes personal data on behalf of the data controller.</td>
</tr>
</tbody>
</table>
Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

The Data Controller

Brentside High School processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

- **Governing Body:** The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
- **Data protection officer:** 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.

The DPO will provide an annual report of their activities directly to the governing body and, where relevant, report to the body their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. Details of the DPO’s responsibilities are set out in their job description.

The DPO for Brentside High is:

<table>
<thead>
<tr>
<th>DPO</th>
<th>Craig Stilwell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Judicium Consulting Ltd</td>
</tr>
<tr>
<td></td>
<td>72 Cannon Street</td>
</tr>
<tr>
<td></td>
<td>London</td>
</tr>
<tr>
<td></td>
<td>EC4N 6AE</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:dataservices@judicium.com">dataservices@judicium.com</a></td>
</tr>
<tr>
<td>Telephone</td>
<td>0203 326 9174</td>
</tr>
</tbody>
</table>

- The Headteacher acts as the representative of the data controller and delegates’ responsibility to the Safeguarding Officer and the School Business Manager on a day-to-day basis.

- All 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 for example; 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
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - 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

Data Protection Principles
GDPR is based on data protection principles that our school must comply with. The principles say 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

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

Collecting Personal Data

Lawfulness, Fairness and Transparency
We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

1. 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 into a contract
2. The data needs to be processed so that the school can comply with a legal obligation
3. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life
4. 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
5. 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)
6. The individual (or their parent/carer when appropriate in the case of a student) has freely given clear consent. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Limitation, Minimisation and Accuracy
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.

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 where necessary.

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. This will be done in accordance with the law and will follow best practice guidelines as set out in the Information and Records Management Society’s toolkit for schools.

Sharing Personal Data
We will not share personal data with anyone else, but may do so when:

- 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 will 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. When doing this, we will:
  o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  o 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

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

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.

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

**Subject access requests and other rights of individuals**

**Subject Access Requests**

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

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

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

If staff receive a subject access request they must immediately forward it to the DPO.
Students and Subject Access Requests
Personal data about a student belongs to that student, and not the student's parents or carers. For a parent or carer to make a subject access request with respect to their student, the student must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Students 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, most subject access requests from parents or carers of students at our school may not be granted without the express permission of the student. This is not a rule and a student’s ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests
When responding to requests, we:

- May ask the individual to provide 2 forms of identification one of which will be photo ID (Passport or Driving licence)
- 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

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 student is at risk of abuse, where the disclosure of that information would not be in the student’s best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the student

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.

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 collecting personal data), 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 on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- 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)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

**Parental Requests to see the Educational Record**
Parents, or those with parental responsibility, have a legal right to free access to their student’s educational record (which includes most information about a student) within 15 school days of receipt of a written request.

**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 and accompanied by prominent signs explaining that CCTV is in use. 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 via the student information form from parents/carers for photographs and videos to be taken of their student for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Uses may include:
• To record and celebrate achievement
• Within school on notice boards and in school magazines, brochures, newsletters, etc.
• Outside of school by external agencies such as the school photographer, newspapers, campaigns
• Online on our school website 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 any other personal information about the student, to ensure they cannot be identified.

See our Acceptable Use Policy for more information on our use of photographs and videos.

**Data Protection by Design and Default**
We will put measures in place to show that we have integrated data protection into all of 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 high 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:
  o For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  o 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

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 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 anywhere else where there is general access
• Where personal information needs to be taken off site, staff must sign it in and out from the school office
• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are automatically reminded to change their passwords at regular intervals
• A remote in facility is used to reduce the need to transport data. Encrypted sticks are used when data needs to be transported.
• Staff, 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 our acceptable use agreement)
• 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 adequately protected (see sharing personal data)

Disposal of Records
Personal data that is no longer needed will be disposed of securely. 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 or incinerate paper-based records, and overwrite or delete electronic files. 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.

Personal Data Breaches
The school will make all reasonable endeavours to ensure that there are no personal data breaches. 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 a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the student premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students

**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 make it necessary.

**Monitoring Arrangements**
The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school’s practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board.

**Links with other policies**
This data protection policy is linked to our:

- Freedom of information policy
- Acceptable use Policy
- IT Security Policy
- E-Safety Policy
- Remote Access and Acceptable Use Policy
- Mobile Phone & Technology Policy
- Student Protection & Safeguarding Policy
Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. 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
- The DPO will alert the Headteacher and the chair of governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the 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
  - Identify theft or fraud
  - Financial 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

If it’s likely that there will be a risk to people’s rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in a secure area of the school’s network.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
• The name and contact details of the DPO
• A description of the likely consequences of the personal data breach
• A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

• The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
• The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  o Facts and cause
  o Effects
  o Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school’s computer system.

• The DPO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Example: Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the School’s IT Support Provider to recall it
• In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
Appendix 2

Privacy Notice for Brentside High School

Brentside High School is committed to protecting the privacy and security of personal information. This privacy notice describes how we collect and use personal information about students, in accordance with the General Data Protection Regulation (GDPR), section 537A of the Education Act 1996 and section 83 of the Children Act 1989.

Who Collects This Information

Brentside High School is a “data controller.” This means that we are responsible for deciding how we hold and use personal information about students.

The Categories of Student Information, What We Collect, Process, Hold and Share

We may collect, store and use the following categories of personal information about you (please note this is not an exhaustive list):

- Personal information such as name, student number, date of birth, gender and contact information
- Emergency contact and family lifestyle information such as names, relationship, phone numbers and email addresses
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance details (such as sessions attended, number of absences and reasons for absence)
- Financial details as necessary
- Post 16 learning information
- Performance and assessment information
- Behavioural information (including exclusions)
- Special educational needs information
- Relevant medical information
- Special categories of personal data (including biometric data, ethnicity, relevant medical information, special educational needs information)
- Images of students engaging in school activities and may be used in a number of media platforms, including but not limited to print, digital and electronic use by Brentside High School for marketing and development purposes
- Images captured by the School’s CCTV system
- Information about the use of our IT, communications and other systems, and other monitoring information
- Safeguarding information

Collecting 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 the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes.

How We Use Your Personal Information

We hold student data and use it for:

- Student selection (and to confirm the identity of and to communicate with prospective students and their parents)
- Providing education services and extra-curricular activities to students, and monitoring students' progress and educational needs
- Informing decisions such as the funding of schools
- Assessing performance and to set targets for schools
- Safeguarding students' welfare and providing appropriate pastoral (and where necessary medical) care
- Support teaching and learning
- Giving and receive information and references about past, current and prospective students, and to provide references to potential employers of past students
- Managing internal policy and procedure
- Enabling students to take part in assessments, to publish the results of examinations and to record student achievements
- To carry out statistical analysis for diversity purposes
- Legal and regulatory purposes (for example student protection, diversity monitoring and health and safety) and to comply with legal obligations and duties of care
- Enabling relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate
- Monitoring use of the school's IT and communications systems in accordance with the school's IT security policy
- Making use of media images of students in school publications, on the school website, on social media channels, for school trips and activities
- Security purposes, including CCTV
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school
- To provide support to students after they leave the school
- To provide support to students in organising work experience activities

**The Lawful Basis on Which We Use This Information**

We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- **Public task:** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and
- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- **Vital interests:** the processing is necessary to protect someone’s life.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is require or permitted by law.

**Sharing Data**

We may need to share your data with third parties where it is necessary. There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it’s the only way we can make sure you stay safe and healthy or we are legally required to do so.
We share student information with:

- the Department for Education (DfE) - on a statutory basis under section 3 of The Education (Information About Individual Students) (England) Regulations 2013
- Ofsted
- Youth support services – under section 507B of the Education Act 1996, to enable them to provide information regarding training and careers as part of the education or training of 13-19 year olds
- Other Schools that students have attended/will attend
- NHS
- Welfare services (such as social services)
- Law enforcement officials such as police, HMRC
- Local Authority
- Professional advisors
- Support services (including insurance, IT support, information security); and
- Catering and Premises Services where relevant
- Third party software packages that support the school in delivering services

Information will be provided to those agencies securely or anonymised as necessary.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

If you relocate outside of the EU, you would need to provide specific instructions to the school to share any student data with any organisation for example an educational institution. Please contact the school should you require this service.

**Why We Share This Information**

We do not share information about our students with anyone without consent unless otherwise required by law.

For example, we share student’s data with the DfE and the local authority on a statutory basis which underpins school funding and educational attainment. To find out more about the data collection requirements placed on us by the DfE please go to [https://www.gov.uk/education/data-collection-and-censuses-for-schools](https://www.gov.uk/education/data-collection-and-censuses-for-schools).

**Storing Student Data**

Brentside High School will keep information about students on computer systems and in manual filing systems. Except as required by law, the school only retains information about students for as long as necessary in accordance with timeframes imposed by law and our internal policy. All confidential data is disposed of in line with the school’s confidentiality policy.

If you require further information about our retention periods, please email info@brentsidehigh.ealing.sch.uk to request a copy of our policy.

**Automated Decision Making**

Automated decision making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision making in limited circumstances.
Sixth Form Admissions Applications

Please note that although student information is sorted by an electronic system each student is interviewed before an admissions offer is made.

Students will not be subject to automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way).

Youth Support Services

Students aged 13+

Once our students reach the age of 13, we also pass student 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.

We must provide the students’ name, the parents’ name(s) and any further information relevant to the support services role.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that only their student’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 student/student once he/she reaches the age 16.

Students aged 16+

We will also share certain information about students 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 website.

The National Student Database

The NPD is owned and managed by the Department for Education and contains information about students 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 students 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 Students) (England) Regulations 2013.


The department may share information about our students 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 student 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 student information, (and for which project), please visit the following website:

https://www.gov.uk/government/publications/national-student-database-requests-received

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

**Requesting Access to Your Personal Data**

Under data protection legislation, parents and students 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 student’s education record], contact info@brentsidehigh.ealing.sch.uk

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 purposes 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.
We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

**Right to Withdraw Consent**

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, contact info@brentsidehigh.ealing.sch.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Contact**

If you would like to discuss anything within this privacy notice or have a concern about the way we are collecting or using your personal data, we request that you raise your concern with info@brentsidehigh.ealing.sch.uk in the first instance.

We have appointed a data protection officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolve by Brentside High School, then you can contact the DPO on the details below:

Data Protection Officer Name: Craig Stilwell, Data Protection Officer Details: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE, Data Protection Officer Email: dataservices@judicium.com

You have the right to make a complaint at any time to the Information Commissioner’s Office, the UK supervisory authority for data protection issues at https://ico.org.uk/concerns.

**Changes to This Privacy Notice**

We reserve the right to update this privacy notice at any time. The privacy notice will be available via the schools website and we will notify you when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

By completing and signing the below table you are agreeing to Brentside High School privacy notice.

<table>
<thead>
<tr>
<th>Name of Parent</th>
<th>Signed by Parent</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Student</td>
<td>Signed by Student</td>
<td>Date</td>
</tr>
</tbody>
</table>