



Brighter Futures
Educational Trust

PRIVACY NOTICES STUDENTS POLICY

Policy Number: 36

Review Committee: Finance and Risk

Type of Policy: Statutory

Review Period: Annually

Approved: November 2025

Next Review: November 2026

VERSION CONTROL

V1.1	June 2024	Version control added Names/roles changed
V1.2	November 2025	New layout due to rebrand

CONTENTS

1. Data protection principles
2. Why do we collect and use student information
3. Statutory functions
4. Student information that we collect, hold and share
5. Collecting student information
6. Storing student data
7. Data sharing
8. Why do we share student information
9. Aged 14+ qualifications - Brandles only
10. Youth support services - student Ages 13+ - Brandles only
11. Data collection requirements
12. The national student database (NPD)
13. Data security
14. Rights of access, correction, erasure and restriction
15. Fees
16. What we may need for you
17. Right to withdraw consent
18. Compliance
19. Changes to this privacy notice

1. DATA PROTECTION PRINCIPLES

We will comply with data protection law. This says that the personal information we hold about you must be:

- a) Used lawfully, fairly and in a transparent way.
- b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- c) Relevant to the purposes we have told you about and limited only to those purposes.
- d) Accurate and kept up to date.
- e) Kept only as long as necessary for the purposes we have told you about.
- f) Kept securely.

2. WHY DO WE COLLECT AND USE STUDENT INFORMATION

We collect and use student information under section 537A of the Education Act 1996, section 83 of the Children Act 1989, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

We collect and use pupil information under the following lawful bases under the UK General Data Protection Regulation (UK GDPR):

We collect and use student information under the following lawful bases:

- a) Where we have the consent of the data subject (Article 6 (a)).
- b) Where it is necessary for compliance with a legal obligation (Article 6 (c)).
- c) Where processing is necessary to protect the vital interests of the data subject or another person (Article 6(d)).
- d) Where it 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 (Article 6 (e)).

Where the personal data we collect about students is sensitive personal data, we will only process it where:

- a) We have explicit consent [Article 9 (2)(a)]
- b) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Article 9 (2)(c)]; and /or
- c) Processing is necessary for reasons of substantial public interest and is authorised by UK law (see section 10 of the 2018 Data Protection Act) [Article 9 (2)(g)].

3. STATUTORY FUNCTIONS

We use the student data to support our statutory functions of running a school, in particular:

- a) To decide who to admit to each school.
- b) Support student learning.
- c) Monitor and report on student progress.
- d) Provide appropriate pastoral care.
- e) Assess the quality of our services.
- f) Comply with the law regarding data sharing.
- g) For the protection and welfare of students and others in each school, including our safeguarding/ child protection obligations.
- h) For the safe and orderly running of each school.
- i) To promote each school.
- j) Communicate with parents / carers.
- k) Send you communications that may be of interest to you which may include information about school events or activities, news, campaigns, appeals, other fundraising activities.
- l) To respond to investigations from our regulators or to respond to complaints raised by our stakeholders.
- m) On connection with any legal proceedings threatened or commenced against each school.

4. STUDENT INFORMATION THAT WE COLECT, HOLD AND SHARE

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). Student information is anonymous when presented to external agencies or reports to Trustees/ Governors.

There are “special categories” of more sensitive personal data which require a higher level of protection. The categories of student information that we collect, hold and share include:

- a) Personal information (such as name, unique student number and address).
- b) Characteristics (such as ethnicity, language, medical conditions, nationality, country of birth and free school meal eligibility).
- c) Attendance information (such as sessions attended, number of absences and absence reasons).
- d) Assessment information (such as examination results and progress reports).
- e) Medical information (such as existing medical conditions, prescribed medication and allergies).
- f) Special Educational Needs information (such as diagnosed needs, non-diagnosed needs, level of need and strategiesto help with the need).
- g) Behavioural information (such as behaviour logs form members of staff, consequences,

rewards and detentions).

- h) Exclusion information (such as fixed term and permanent exclusions).
- g) Curriculum information (such as timetables and subjects studied).

From time to time and in certain circumstances, we might also process personal data about students, some of which might be sensitive personal data, including information about criminal proceedings / convictions, information about sex life and sexual orientation, child protection / safeguarding. This information is not routinely collected about students and is only likely to be processed by the school in specific circumstances relating to particular students, for example, if a child protection issue arises or if a student is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and/ or the Police. Such information will only be processed to the extent that it is lawful to do so, and appropriate measures will be taken to keep the data's secure.

5. COLLECTING STUDENT INFORMATION

We collect information about students when they join each school and update it during their time on the roll and when new information is acquired.

Whilst the majority of student information provided to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK GDPR, we will inform you whether you are required to provide certain student information to us or if you have a choice in this. Where appropriate, we will ask parents/students for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to use photos or images of students on our website or on social media to promote school activities or if we want to ask your permission to use your information for marketing purposes. Parents/students may withdraw consent at any time.

When students are deemed to be old enough to make their own decisions in relation to their personal data, we will also ask the student for their consent in these circumstances. This will usually be around the age of 13. Although parental consent is unlikely to be needed, we wish to take a collaborative approach so we will keep parents informed when we are approaching students for consent up to the age of 18. Students with the maturity to make their own decisions about their personal data may withdraw consent if consent has previously been given.

In addition, each school also uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving students will only be processed to the extent that it is lawful to do so.

6. STORING STUDENT DATA

We hold your data securely and have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. Access to information is limited to those who have a business need to know it and who are subject to a duty of confidentiality. A significant amount of personal data is stored electronically, for example, on our Behaviour Watch databases. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud-based system. We have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach involving your data where we are legally required to do so.

When a student moves to another educational setting or school phase, the vast majority of information that we hold will move to that setting, although we may need to retain a certain amount of personal data.

Where we act as the final setting in a student's education, we are required to retain some personal information for a period after they have left. Please refer to the school's Data Retention Schedule for retention periods. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

7. DATA SHARING

We share student data with third parties, including third-party service providers and other organisations. In particular, we may share student data with organisations including, but not limited to, those detailed below.

We routinely share student information with:

- Schools within the trust
- Schools that students attend after leaving us.
- The local authority, Hertfordshire County Council.

- A student's home local authority (if different).
- The Department for Education (DfE).
- Trust and Governors
- Exam boards.
- Our payment processing system for school lunches and visits/trips.
- CPOMs, for child protection, safeguarding, pastoral and welfare purposes.
- The schools' Management Information Systems.
- Google platforms and the schools' remote learning platforms.
- Wonde, as a secure data transfer portal.
- Third party educational software/resource providers, where we have completed due diligence on the organisation and data provided is minimal and non-sensitive.

From time to time, we may also share student information with other third parties including the following:

- Police and law enforcement agencies.
- NHS health professionals including a school nurse and educational psychologists,
- Education Welfare Officers.
- Courts, if ordered to do so.
- Colleges
- Prevent teams in accordance with the Prevent Duty on schools.
- Other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances.
- HR providers, for example, if we are seeking HR advice and a student is involved in an issue.
- UCAS.
- Our IT, legal and insurance providers and auditors.
- Office365, email and apps.

Some of the above organisations may also be data controllers in their own right in which case we will be joint controllers of your personal data and may be jointly liable in the event of any data breaches.

We may also share student data with a number of providers of software tools which may be used to: support student learning; monitor and report on student attainment and progress; deliver the educational curriculum; ensure the safety and wellbeing of students; communicate with parents; or to carry out other operational processes to support our core activities as a public authority, under Article 6(e) of the UK GDPR. These providers act as data processors on our behalf and are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow them to use your personal data for their own purposes, and we only permit them to process your personal data for specified purposes and in accordance with our instructions.

In the event that we share personal data about students with third parties or data processors, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

8. WHY DO WE SHARE STUDENT INFORMATION

We do not share information about our pupils with anyone without consent unless the law allows 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 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

9. AGED 14+ QUALIFICATIONS – BRANDLES ONLY

For students enrolling for post 14 qualifications, the information you supply is used by the Learning Records Service (LRS). The LRS issues Unique Learner Numbers (ULN) and creates Personal Learning records across England, Wales and Northern Ireland, and is operated by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE). The LRS will give us a student's ULN and may also give us details about the student's learning or qualifications. For more information about how your information is processed, and to access your Personal Learning Record, please refer to:

<https://www.gov.uk/government/publications/lrs-privacy-notice/lrs-privacy-notice#tier-2-privacy-notice-text>

10. YOUTH SUPPORT SERVICES – STUDENT AGES 13+ BRANDLES ONLY

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.

This enables them to provide services as follows:

- youth support services.
- careers advisors.

A parent / 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/student once he/she reaches the age 16.

11. DATA COLLECTION REQUIREMENTS

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 (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

12. THE NATIONAL STUDENT DATABASE (NPD)

The NPD is owned and managed by the DfE 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. To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

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 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 DfE 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-collectandshare-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>.

13. DATA SECURITY

We have put in place measures to protect the security of personal information.

Third parties who are processing personal data on our behalf will only process personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal information to those third parties who have a business need to know. They will only process personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so

14. RIGHTS OF ACCESS, CORRECTION, ERASURE AND RESTRICTION

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

Under certain circumstances, by law you have the right to request access to your personal information: Under data protection legislation, students, and in some circumstances, parents, have the right to request access to information about them that we hold ("Subject Access Request"). From the age of 13, we generally regard students as having the capacity to exercise their own rights in relation to their personal data. This means that where we consider a student to have sufficient maturity to understand their own rights, we will require a Subject Access Request to be made by the student and not their parent(s) on their behalf. This does not affect any separate statutory right parents might have to access information about their child.

Subject to the section below, the legal timescales for the school to respond to a Subject Access Request is one calendar month. As each school has limited staff resources outside of term time, we encourage parents / students to submit Subject Access Requests during term time and to avoid sending a request during periods when the school is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible.

Parents of students who attend academies have a separate statutory right to receive an annual written report setting out their child's attainment for the main subject areas which are taught. This is an independent legal right of parents rather than a student's own legal right which falls outside of the UK GDPR, therefore a student's consent is not required even a student is able to make their own decisions in relation to their personal data, unless a court order is in place which states otherwise.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the student, with whom the student lives or whether the student has contact with that parent), and also includes non-parents who have parental responsibility for the student, or with whom the student lives. It is therefore possible for a student to have several "parents" for the purposes of education law.

- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have

exercised your right to object to processing (see below).

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.
- If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

15. FEES

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

16. WHAT WE MAY NEED FROM YOU

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.

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 our data protection responsibilities.

We will always seek to comply any requests regarding your rights, however, please note that we may still be required to hold or use your information to comply with legal duties.

For further information about your rights, including the circumstances in which they apply, see the [guidance](#) from the Information Commissioners Office (ICO) on individuals' rights under the UK GDPR.

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

17. RIGHT TO WITHDRAW CONSENT

In the limited 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 anytime. To withdraw your consent, please contact Carole Connelly, the school's DPO.

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.

18. COMPLIANCE

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO, Carole Connelly email: carole@schooldposervice.com

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

19. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice 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.