

Bourne Education Trust

Pupil/Parent Privacy Notice

Privacy Notice: how we use pupil and parent/carers information

The purpose of this notice is to give pupils and their parent(s)/carer(s) information on how personal data is used in our educational settings.

Data controller and processors

Each academy within Bourne Education Trust (BET) is the Data Controller for the purposes of data protection law, determining the purposes for which personal data is used (processed). Authorised third parties process the data on behalf of the academies and are therefore data processors.

The categories of personal data that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address and contact details of parents/carers)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment information (such as key stage 1 results and phonics results, post 16 courses enrolled for and any relevant results)
- Special educational needs information (including the needs and ranking)
- Relevant medical and administration information (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Safeguarding information (such as court orders and professional involvement)
- Post 16 learning and vocational information (where relevant)
- Other, including photographs, trip administration, catering and free school meal management, CCTV images captured on academy properties and biometric data (in certain academies)

Why we collect and use this information

We collect and use this data under legal and statutory obligations within the Education Act 1996; The Children Act 2004; Education and Inspections Act 2006; Education Act 2011; the Children and Families Act 2014.

We collect and use pupil data for the following purposes:

- To support pupil learning

- To monitor and report on pupil attainment progress
- To provide appropriate pastoral care
- To assess the quality of our services
- To comply with the law regarding data sharing
- To safeguard pupils
- To provide academic, examination and career references for pupils and staff
- To fulfil the Academy's and the Trust's contractual and other legal obligations
- To administer admissions waiting lists
- To contact pupils and parents/carers when we need to.
- To meet the statutory duties placed upon us for the Department of Education (DfE) data collections.

The lawful basis on which we use this information

We collect and use (process) pupil information where:

- We need to comply with a legal obligation
- We need to perform an official task in the public interest – for example to provide a pupil with an education.

We may also use a pupil's or parent/carer's information where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's health interests (or someone else's interest).

The legal basis for processing personal data under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 will be one of the following:

- Article 6(1)c: processing is necessary for compliance with a legal obligation to which the controller is subject, or
- Article 6(1)e: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The legal basis for processing special categories of data under UK GDPR and Data Protection Act 2018 will be one of the following:

- Article 9(2)g: processing is necessary for reasons of substantial public interest on the basis of Union or Member State law
- Article 9(2)h: processing is necessary for the provision of health or social care systems and services on the basis of Union or Member State law.

Where we have obtained consent to use a pupil's or parent/carer's personal data, the consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Collecting pupil information

We collect pupil information via registration forms when your child joins the school, and via a Common Transfer File (CTF) or secure file transfer from the previous school.

Pupil data is essential for schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply

with the data protection legislation, we will inform you at the point of collection 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 securely for the periods of time recommended in the Information and Records Management Society (IRMS) Schools Toolkit: IRMS Schools Toolkit, or as stated in our Data Retention Policy if different.

We use a range of software and hardware measures and controls, and staff training, to ensure that the data we hold is secure and protected.

The following policies support our commitment to safe use of data within our academies and can be found [here](#):

- BET Data Protection Policy
- BET CCTV policy
- BET Website Conversational AI privacy notice
- BET Data Retention Policy

Who we share pupil information with:

We routinely share pupil information with:

- Schools and colleges that pupils attend after leaving us
- Our local authority, including the Education Welfare Officer or specialist consultant advising on attendance
- The Department for Education (DfE)
- Agencies such as the Standards and Testing Agency, Ofsted, the Department of Health and Social Care, the Police and Social Services
- Youth support services (pupils aged 13+)
- Bourne Education Trust
- The National Health Service (for routine health checks and vaccinations undertaken in schools)
- Educational software providers for services to enhance the curriculum
- Educational consultancies providing specialist support, for example with analysis of attendance data.

These bodies act as data controllers in respect of the data they receive and are subject to the same legal constraints in how they deal with the data.

Why we regularly 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 pupil information for the following purposes:

- To support transitions to schools and colleges that pupils attend after leaving us and meet our statutory safeguarding duties
- To support shared statutory duties with our local authority, including the Education Welfare Officer or specialist consultant advising on attendance and to safeguard children and young people.

- To meet our statutory duties to the Department of Education and other agencies such as the Standards and Testing Agency, Ofsted, the Department of Health and Social Care, the Police and Social Services and to safeguard children and young people.
- To enable youth support services (pupils aged 13+) to perform their responsibilities under section 507B of the Education Act 1996.
- To support internal benchmarking and best practice sharing across the Bourne Education Trust.
- To enable the National Health Service to undertake their routine health checks and vaccinations within schools.
- To enhance the curriculum through services from educational software providers.
- To access specialist support to improve the analysis of pupil data such as attendance.

Data is transferred electronically via encrypted software.

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

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.

Data is securely transferred to the youth support service via a combination of software and hardware controls and is stored in line with the IRMS Toolkit for Schools or our Data Retention Policy where different.

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

Data is securely transferred to the youth support service via a combination of software and hardware controls and is stored in line with the IRMS Toolkit for Schools or our Data Retention Policy where different.

For more information about services for young people, please visit the local authority website: Surrey County Council Schools and Learning.

Operation Encompass

BET schools are enrolled onto the Operation Encompass scheme, a joint project between police forces, local authorities, LA Domestic Abuse Services and schools, where every school day morning DSLs are notified of all domestic abuse incidents that have occurred and been reported to police in the previous 24 hours which involved a child at school (72 hours on a Monday morning). This provides an opportunity for schools to ensure the right support is in place at the right time for children who are experiencing domestic abuse. For more information on Operation Encompass, please visit: [Home : Operation Encompass](#) .

Department for Education (DfE)

The DfE collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the DfE either directly or via our local authority for the purpose of those data collections.

We share pupil 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.

Pupil Referral Units are required to pass information about pupils to the Department for Education (DfE) under regulation 4 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by the DfE under a combination of software and hardware controls which meet the current government security policy framework - [Security policy framework: protecting government assets - GOV.UK](#).

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 [Data collection and censuses for schools - GOV.UK \(www.gov.uk\)](#) and see the “How Government uses your data” section later in this document.

Requesting access to your personal data

Under data protection legislation, parent(s)/carer(s) and pupils have the right to request access to the information about them that we hold. To make a request for your personal information, contact the Headteacher of your child’s school, as outlined in the Bourne Education Trust’s

Data Protection Policy. Where possible, this information will be made available, but as an Academy, it is at the school's discretion whether or not educational records are made available.

You also have the following rights:

- the right to be informed about the collection and use of your personal data – this is called 'right to be informed'.
- the right to ask us for copies of your personal information we have about you – this is called 'right of access', this is also known as a subject access request (SAR), data subject access request or right of access request.
- the right to ask us to change any information you think is not accurate or complete – this is called 'right to rectification'.
- the right to ask us to delete your personal information – this is called 'right to erasure'
- the right to ask us to stop using your information – this is called 'right to restriction of processing'.
- the 'right to object to processing' of your information, in certain circumstances
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner's Office (ICO) if you feel we have not used your information in the right way.

There are legitimate reasons why we may refuse your information rights request, which depends on why we are processing it. For example, some rights will not apply:

- right to erasure does not apply when the lawful basis for processing is legal obligation or public task.
- right to portability does not apply when the lawful basis for processing is legal obligation, vital interests, public task or legitimate interests.
- right to object does not apply when the lawful basis for processing is contract, legal obligation or vital interests. And if the lawful basis is consent, you don't have the right to object, but you have the right to withdraw consent.

If you have a concern or complaint about the way we are collecting or using your personal data, we request that you raise your concern with the school in the first instance. Please see the BET Data Protection Policy for more details on this process. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

For further information on how to request access to personal information held centrally by the DfE, please see [Appendix A](#).

Recording of lessons/meetings

Many devices in use in schools have the ability to produce an audio or video recording, and the use of video conferencing platforms with recording ability is commonplace.

Meetings, such as might occur between members of staff, or between a member of staff and a parent/carers or pupil will not be recorded. Recordings collect personal data, so must comply with Article 5 of GDPR: data collected must be limited to 'what is necessary'. It is normally

sufficient to have a note taker minute a meeting if a record is required. Where there is disagreement over the minutes taken, the disagreeing party should annotate a copy of the disputed minutes and both parties should retain a copy of the annotated minutes for reference. Article 5 also requires that any recording is stored securely, kept only as long as necessary, has limited access and that the recording is processed lawfully, fairly and in a transparent manner. If a meeting recording were to be shared by either party or made public without their consent, this would likely be in breach of GDPR, potentially resulting in a complaint to the Information Commissioner's Office.

An exception may be made, for example, when a meeting participant's first language is not English, or when recording a meeting is a reasonable adjustment in light of a participant's disability.

Lessons delivered online are routinely recorded using proprietary tools such as Microsoft Teams. Recordings of online lessons are made to safeguard all participants, who are advised of the recording at the start of each session. Individuals refusing permission to be recorded are prevented from participating in that session. Recordings are stored securely within Microsoft Teams and Stream and are only available to participants. Recordings are retained in accordance with the [BET Data Retention policy](#).

Filtering and Monitoring

To help keep pupils safe online and meet our safeguarding responsibilities, Bourne Education Trust (BET) uses Lightspeed Filtering and Alert on all Trust-managed devices and networks, including computers, Chromebooks, iPads and internet services.

We monitor device activity, internet usage, application usage and security-related events. The system may also identify online activity, searches, keywords and patterns of use that indicate potential safeguarding concerns, such as bullying, self-harm, extremism or other risks to pupil welfare.

Monitoring information may be reviewed by authorised staff, including the Trust Safeguarding Lead, Designated Safeguarding Leads (DSLs), Deputy DSLs, Headteachers, and Lightspeed Systems where necessary to provide the service. Where a concern is identified, alerts are sent to safeguarding staff for review and, where appropriate, intervention.

We carry out this monitoring to safeguard pupils and staff, protect Trust systems and data, ensure compliance with school policies, and meet our legal duties under safeguarding legislation and Department for Education guidance.

Monitoring data is retained by Lightspeed Systems for up to 90 days before deletion and is handled in accordance with UK GDPR and our Data Protection policies.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting the school directly.

Last updated

We may need to update this privacy notice periodically, so we recommend that you revisit this information from time to time. This version was last updated in August 2026.

Contact

If you would like to discuss anything in this privacy notice, please contact the Headteacher of your child's school in the first instance. Bourne Education Trust's Data Protection Team can be contacted by email: dpo@bourne.education

Published date:	Autumn term 2026
Author:	Head of Compliance
Approved by:	Chief Strategy Officer
Next review:	Autumn 2028

Appendix A: How Government uses your data

The pupil data that we lawfully share with the Department for Education (DfE) through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school
- informs ‘short term’ education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports ‘longer term’ research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (DfE) (for example; via the school census) go to

<https://www.gov.uk/education/data-collection-and-censuses-for-schools>

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

The data in the NPD is provided as part of the operation of the education system and is used for research and statistical purposes to improve, and promote, the education and well-being of children in England.

The evidence and data provide DfE, education providers, Parliament and the wider public with a clear picture of how the education and children’s services sectors are working in order to better target, and evaluate, policy interventions to help ensure all children are kept safe from harm and receive the best possible education.

To find out more about the NPD, go to

<https://www.gov.uk/government/publications/national-pupil-database-npd-privacy-notice/national-pupil-database-npd-privacy-notice>

Sharing by the Department for Education (DfE)

DfE will only share pupils’ personal data where it is lawful, secure and ethical to do so. Where these conditions are met, the law allows the Department for Education (DfE) to share pupils’ personal data with certain third parties, including:

- schools and local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department for Education’s (DfE) NPD data sharing process,

please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

Organisations fighting or identifying crime may use their legal powers to contact the Department for Education (DfE) to request access to individual level information relevant to detecting that crime.

For information about which organisations the Department for Education (DfE) has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website:

<https://www.gov.uk/government/publications/dfe-external-data-shares>

How to find out what personal information the Department for Education (DfE) holds about you

Under the terms of the UK GDPR, you are entitled to ask the Department for Education (DfE):

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department for Education (DfE), you should make a 'subject access request'. Further information on how to do this can be found within the Department for Education's (DfE) personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter> or

<https://www.gov.uk/government/publications/requesting-your-personal-information-from-dfe#your-rights>

To contact the Department for Education (DfE): <https://www.gov.uk/contact-dfe>