



Privacy Notice Staff

Autumn 2025

Approved by: Governing Body

Autumn 2025

Last reviewed:

Autumn 2025

Next review due by:

Autumn 2026

Privacy Notice (How we use school workforce information)

This notice explains what personal data (information) we hold about you, how we collect, how we use and may share information about you. We are required to give you this information under data protection law.

We, Haydon Abbey School and Pre-School, Weedon Road, Aylesbury, HP19 9NS, 01296 482278 are the 'data controller' for the purposes of UK data protection law.

Our data protection officer is Tracey Adams (see 'Contact us' below).

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

- personal information (such as name, employee or teacher number, national insurance number)
- special categories of data including characteristics information such as gender, age, ethnic group and trade union membership
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information
- contact information including address, email and phone numbers
- payroll information
- DBS information
- Information relation to trade union membership

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- safeguarding and child protection including KCSiE 2024 filtering and Monitoring
- Inform financial audits of the school
- Fulfil our duty of care towards our staff
- Inform national workforce policy monitoring and development
- to undertake education research and share data (teacher training schools)

The lawful basis on which we process this information

We rely on having a legitimate reason as your employer to collect and use your personal information, and to comply with our statutory obligations, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of contract, legal obligation (not including contractual obligation), substantial public interest (equality of opportunity or treatment) or vital interest (to protect someone's life) found in [UK GDPR Article 9](#).

We are required to share information about our workforce members under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Collecting this information

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

Storing this information

We hold staff / employee data in line with [IRMS Toolkit](#) (Information records management service) guidelines data storage including time scales.

We have put in place appropriate security measures to prevent your personal information being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

Who we share this information with

We routinely share this information with:

- **Buckinghamshire Council**
- Government departments or agencies
- Department for Education (DfE)
- **Buckinghamshire Council Schools Financial Services**
- Commissioned providers of personnel and payroll services Buckinghamshire Council
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts or tribunals

Why we share school workforce information

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

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

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

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

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and

Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

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

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

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

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit:

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

To contact the department: <https://www.gov.uk/contact-dfe>

The Lawful Basis for processing personal data

The lawful bases for processing personal information are:

- In accordance with the 'public task' basis to process data to fulfil our official duties
- in accordance with the 'legal obligation' basis to process data to meet our responsibilities
- In accordance with the 'consent' basis we will get consent from you to use your personal data
- In accordance with the 'vital interests' basis we will use this personal data in a life-or-death situation
- In accordance with the 'contract' basis we need to process personal data to fulfil a contract with you or to help you enter into a contract with us
- In accordance with the 'legitimate interests' basis where there's a minimal privacy impact and we have a compelling reason, including

The Lawful Basis for processing special category data

The lawful bases for processing 'special category' data collected (more sensitive personal information) use the following conditions for processing as set out in UK data protection law:

- We obtained your explicit consent to use your information in a certain way
- We need to use your information under employment, social security or social protection law

- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The information has already been made obviously public by you
- We need to use it to make or defend against legal claims
- We need to use it for reasons of substantial public interest as defined in legislation
- We need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law
- We need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made obviously public by you
- We need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims

We need to use it for reasons of substantial public interest as defined in legislation

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also 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 where we are legally required to do so.

Requesting access to your personal data

Under data protection legislation, staff 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 employees records. In the first instance please contact the school Data Protection Lead in the 'contact us' section below.

Access personal information that we hold about you

You have a right to make a 'Subject Access Request' to gain access to personal information that we hold about you and we will (subject to any exemptions that may apply):

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with

- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances such as verified representation.

Your other data rights

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you 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 and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Withdraw your consent, where you previously provided it for the collection, processing and transfer of your personal data for a specific purpose
- In certain circumstances, be notified of a data breach
- Make a complaint to the Information Commissioner's Office
- Claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance using the 'contact us details below.

Alternatively, you can contact the Information Commissioner's Office at

<https://ico.org.uk/concerns/>

Other policies which may reference this privacy notice

This Privacy Notice also applies in addition to the School's/trusts other relevant terms and conditions and policies, including:

- any contract between the School and its staff or the parents of students;
- the School's policy on taking, storing and using images of students;
- the School's policy on the use of CCTV;
- the School's retention of records policy, (IRMS template);
- the School's safeguarding and pastoral policy
- the School's Health and Safety policy, including how concerns or incidents are recorded;
- the School's IT policies, including its Acceptable Use policy, On-line Safety policy

Further information

Contact

If you would like to discuss anything in this privacy notice, In the first instance please contact the School Data Protection Lead below:

Position	Name	Email	Phone
School Data Protection Lead	Tracey Adams, Business Manager	tracey@haydonabbey.bucks.sch.uk	01296 482278
Data Protection Officer	Turn IT on	dpo@turniton.co.uk	01865 597620 (option 3)

Complaints

If you have a complaint, we ask that you raise this with us in the first instance. Under the Data Usage and Access Act 2025, a complaint should be investigated thoroughly by the company first. Should the outcome conclude escalation is required, the Information Commissioners Office will be informed. To raise a complaint, please email: dpo@turniton.co.uk or call 01265 537 620 (option 3)

Should you still wish to contact the ICO, you can do so at <http://ico.org.uk/concerns/> or call 0303 123 1113

Policy update information (policy number GDPR-102)

This policy is reviewed annually and updated in line with data protection legislation.

Policy review information

Review date	Reviewed by
02-05-2018	turn IT on
08-08-2019	turn IT on
04-08-2020	turn IT on
02-08-2021	turn IT on
04-08-2022	turn IT on
01-08-2023	turn IT on
01-08-2024	turn IT on
01-08-2025	turn IT on

Policy update information

Review date	Revision	Description on change	By
02-05-2018	1.00	Draft release	turn IT on
03-05-2018	1.00	Full release	turn IT on
08-08-2019	1.01	Full release	turn IT on
02-08-2021	1.02	Full release	turn IT on
01-08-2023	1.03	Full release	turn IT on
01-08-2023	1.04	Full release	turn IT on
01-08-2025	1.05	Full release	turn IT on