Staff Privacy Notice (How we use your information) 2025 - 2026

This notice sets out how we use your personal information as your employer or when you apply for a job with us and in particular:

- what personal information we collect;
- what we do with your personal information;
- the legal basis on which we collect and use your personal information;
- how long we keep your personal information;
- how we share your personal information including whether we transfer your personal information outside of the European Economic Area ("EEA"); and
- your rights over your personal information.

The categories of information that we collect, process (use), hold and share include

- personal information (such as name, title, addresses, telephone numbers, and personal email addresses, date of birth, employee or teacher number, National Insurance number);
- special categories of data including characteristics information such as gender, race, ethnic origin, trade union membership;
- marital status and dependants;
- next of kin, emergency contact and death benefit nominee(s) information;
- bank account details, payroll records and tax status information;
- salary, annual leave, pension and benefits information;
- contract information such as start date, leaving date, location of employment or workplace, etc;
- copy of driving licence, passport, birth and marriage certificates, decree absolute;
- recruitment information (including copies references and other information included in a cv or cover letter or as part of the application process);
- qualifications (and, where relevant, subjects taught);
- compensation history;
- performance and appraisal information;
- disciplinary and grievance information;
- secondary employment and volunteering information;
- accident book, first aid records, injury at work and third-party accident information;
- information about convictions/allegations of criminal behaviour.
- evidence of your right to work in the UK/immigration status;
- work absence information (such as number of absences and reasons);
- CCTV images including ANPR data; and
- your image (photograph) for your College ID.

How is this collected?

Most of the information above is collected directly from yourself, for instance, via an application, or if you interact with us via social media. However, some information may be collected from other organisations such as the Department for Education (DfE), your previous employer, Disclosure Barring Service (DBS), etc.

Why we collect and use this information

We use this data:

- for the recruitment process and for carrying our pre-employment checks;
- for checking your identity and right to work in the UK;
- for checking your qualifications;
- to provide awarding organisations (where necessary) with confirmation of your qualifications (for quality assurance purposes);
- for carrying out our role as your employer or potential employer;
- to support and manage employees;
- to gather evidence and any other steps relating to possible grievance or disciplinary matters and associated hearings;
- to enable the development of a comprehensive picture of the workforce and how it is deployed;
- to process payroll, pensions, expenses claims and other financial transactions;
- to make decisions about salary reviews and compensation;
- for conducting performance reviews;
- to maintain the College's accounts and for insurance purposes;
- for dealing with HMRC;
- to allow for better financial modelling and planning;
- to inform the development of recruitment and retention policies;
- for safeguarding students including maintaining the Single Central Record;
- to maintain accident records and to otherwise comply with health and safety legislation;
- for communicating with you and for marketing purposes;
- in the case of use of CCTV, to maintain the security of the College's premises, for preventing and investigating crime and when investigating disciplinary matters, etc (see the College's CCTV Policy for further details);
- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security and preventing malicious software distribution;
- and to otherwise fulfil the College's statutory obligations as an educational institution under the Further and Higher Education Act 1992, the Education Act 1996 and other applicable legislation.

The lawful basis on which we process this information

We are subject to statutory and legal obligations requiring us to process this information. We are also required to process this information to enable us to perform our contractual obligations to you as your employer. In some instances, we are required to process this information as we as a college are performing a task in the public interest (provision of education). In some instances, we may decide to process this information because it is in our legitimate interests to do so.

For some non-core purposes, i.e. not directly related to your employment with us, such as staff surveys, marketing, etc. we require your consent to process your personal information. You can withdraw your consent for this processing at any time; but this could have consequences in terms of us being able to provide those non-core services to you.

Special Category Data

Special category data is personal data which the UK GDPR says is more sensitive, and so needs more protection.

Information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

is Special Category Data.

Processing of Special Category Data is necessary for the College to be able to carry out a task in the public interest (provision of education) and to comply with legal and statutory requirements relating to that provision (in particular, safeguarding), and to be able to perform its obligations in relation to its contract of employment with you, in accordance with Articles 6 and 9 UK GDPR and section 10 and Schedule 1, Part 1 of the Data Protection Act 2018, specifically paragraph 1 (employment, social security and social protection), paragraph 8(1) of Schedule 1, Part 1 (equality of opportunity and treatment), paragraph 16 (support for individuals with a particular disability or medical condition), paragraph 18 (safeguarding of children and of individuals at risk), paragraph 20 (insurance) and paragraph 21 (occupational pensions).

Criminal Offence Data

Processing of Criminal Offence Data is necessary for the College to be able to carry out a task in the public interest (provision of education) and to comply with legal and statutory requirements relating to that provision (in particular, safeguarding), in accordance with Articles 6 and 10 UK GDPR and section 10 and Schedule 1, Part 1 of the Data Protection Act 2018, specifically paragraph 18 (safeguarding of children and of individuals at risk) and paragraph 29 of Schedule 1, Part 3 (consent).

Collecting this information

Workforce data is essential to enable the College to function as a college. 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 information to us or if you have a choice in this.

Storing this information

We hold data securely for the set amount of time shown in our data retention schedule. How long we hold this information for will depend on the type of information that is being held and why it is being held.

For further details, the College's Data Retention Policy is available at available https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

Who we share this information with

We routinely share this information with:

- current, past and prospective employers;
- trade unions and staff associations;
- our local education authority;
- HMRC;
- the Department for Education (DfE);
- Disclosure Barring Service;
- pensions providers;
- awarding organisations;
- End Point Assessment Organisations such as Lantra, TQUK[1] and Skills and Education Group[2];
- Higher Education Statistics Agency ("HESA") (see Appendix A below); and
- Access (a private company, to process payroll).

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 of educational attainment.

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so. 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. For further details, please see also https://www.gov.uk/government/organisations/department-for-education

Data collection requirements (DfE)

The DfE may share information about College 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; and by
- providing information, advice or guidance.

[1] GDPR & Privacy policy.pdf
[2] Protecting your privacy : Skills and Education Group

The DfE 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 the 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 this 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 DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the DfE, please go to https://www.gov.uk/contact-dfe

Why we share your information

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

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you; where it is in the public interest to do so or where it is necessary for the performance of our functions as an education institution. This will, in some circumstances, involve sharing special categories of personal data and, where relevant, data about criminal convictions/allegations.

HESA (Staff)

The Higher Education Statistics Agency Limited (HESA) is the body responsible for collecting and disseminating information about higher education in the UK and the designated data body for England (see https://www.hesa.ac.uk/about for more information).

HESA collects information from higher education providers in the UK at the request of its Statutory Customers (https://www.hesa.ac.uk/about/what-we-do/statutory-customers).

HESA and its Statutory Customers are Controllers of the HESA records under GDPR. HESA's ICO registration number is Z7475057.

HESA's wholly-owned subsidiary company HESA Services Limited may also act as a Controller of the data and provides anonymous or pseudonymised data extracts for research purposes. HESA Services Limited's ICO registration number is Z7899462.

All uses of personal data collected by HESA are described in the Collection Notices at www.hesa.ac.uk/about/regulation/data-protection/notices.

Medical Emergency including Mental Health Emergency

In extreme cases, we may, if we consider it to be in your best interests, share your health information, including mental health information, with emergency services and your next of kin.

Our legal basis for doing so is **Legal Obligation** – for instance, we have obligations to do so under the Health and Safety at Work Act 1974 – and **Vital Interests**, i.e. in the event of an emergency and it is not possible to obtain your consent.

As your health data is also Special Category Data, it also requires further conditions of processing. These are **Vital interests** – similar to the vital interests lawful basis discussed above, this condition may apply in circumstances of life and death. Also, **Employment, Social Security and Social Protection law -** to ensure the health, safety and welfare of the College's staff.

Transferring your personal data outside of Europe

Unless otherwise stated, your information will remain at all times within the UK and or European Economic Area ("EEA"). If we have to transfer your personal data outside the EEA, we will only do so where:

- the recipient or recipient country ensures an adequate level of protection for your personal data;
- the recipient or recipient country is subject to an approved certification scheme or code of conduct with binding and enforceable commitments which amount to appropriate safeguards for your personal data;
- we have put in appropriate safeguards with the recipient or recipient country to protect your personal data such as a data sharing agreement;
- the transfer is permitted by law; or
- you expressly consent to that transfer.

Monitoring of the College network and use of College Wi-Fi

The College uses Smoothwall and Senso to monitor computer use to safeguard staff and students.

Smoothwall is a firewall and web filter used to support digital safety and wellbeing.

Senso is a cloud-based platform for device monitoring and management. Monitoring is 24/7 and also includes use of Teams.

'Safeguarding' is a legal obligation. All organisations that work with or come into contact with children should have safeguarding policies and procedures in place to help them keep children safe.

If you connect to the College network or Wi-Fi using your personal device, or a College-issued device, then your use of the College network and systems will be monitored, for safeguarding purposes.

This also extends to staff working from home, who connect to the College network/ systems using their own personal Wi-Fi on either their College or own personal devices.

The Safeguarding team will be informed of any inappropriate use and in extreme cases, such as, for instance, where child pornography is viewed, downloaded or disseminated, then the police and other appropriate authorities will be informed.

The type of data that Smoothwall and Senso collects is username, date, time, IP address (internal users only) and the site(s) visited.

Any data captured by Smoothwall and Senso will be retained for up to one year. After which, it will be deleted or otherwise destroyed.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the College's Data Protection Officer, Judith Clapham, either by contacting Judith at judith.clapham@askham-bryan.ac.uk or at DataProtection@askham-bryan.ac.uk

You also have the right to:

- have your personal data rectified, if it is inaccurate or incomplete;
- request the deletion or removal of personal data where there is no compelling reason for its continued processing;
- restrict our processing of your personal data (i.e. permitting its storage but no further processing);
- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics;
- not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

For further details please visit the ICO's website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-UK GDPR/individual-rights/

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance by contacting Judith Clapham, either at judith.clapham@askham-bryan.ac.uk or at DataProtection@askham-bryan.ac.uk. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact Judith Clapham, either at judith.clapham@askham-bryan.ac.uk or at DataProtection@askham-bryan.ac.uk

The College is registered with the Information Commissioner's Office ("ICO"). The Registration Number is Z6170811. Renewal of the registration takes place annually on 22 January.

Please also see the Data Protection Policy which is available at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

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 1st September 2025.