

Staff Privacy Notice 2025-26

Responsible Officer:	Executive Director Digital Transformation and MIS
Date:	November 2025
Review date:	November 2028 (unless preceded by legislation)
Procedure available:	Intranet, Website
Approved by:	Executive and Finance & Resources Committee

Staff Privacy Notice

How we use workforce information

Under data protection law, individuals have a right to be informed about how Buckinghamshire College Group uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data and data about you.

We, Buckinghamshire College Group are the 'data controller' for the purposes of data protection law. Our data protection officer is Oliver Roth, Executive Director MIS and Digital Transformation.

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

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- your current status regarding your ability to enter the college e.g. current employee, visitor, etc.
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
- physical / electronic data that may identify your location
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief

Why we collect and use this information

The College needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For all positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to work within the College.

In other cases, the College has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the College to:

- run recruitment and promotion processes
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- ensure effective general HR and business administration, this includes using the data to help test the HR system as appropriate
- provide references on request for current or former employees
- respond to and defend against legal claims
- maintain and promote equality in the workplace

Where the College relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the College processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

The lawful basis on which we process this information

You have some obligations under your employment contract to provide the College with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the College with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the College to enter a contract of employment with you. If you do not provide other information, this will hinder the College's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

The lawful basis on which we process workforce information under Article 6 of GDPR is as follows:

“(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;”

and/or

“(c) 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;”

Where data processed is classified as special category data under GDPR, the lawful basis on which we process workforce information under Article 9 of GDPR is as follows:

“(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;”

We only collect and use workforce personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need to comply with a contractual obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process workforce personal data in situations where:

- We have legitimate interests in processing the data
- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use workforce personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using workforce personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

The College collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the College collects personal data about you from third parties, such as references supplied by former employers, and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the College's HR management system (iTrent) and in other IT systems (including the College's email system, our access management system [iTrent], and OneDrive).

Storing this information

The College takes the security of your data seriously. The College has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the College engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

The College will hold your personal data for the duration of your employment. Your data is held for 7 years after the end of your employment. At the end of that period (or once you withdraw your consent), your data is deleted or destroyed.

When data is stored and/or retained, we will continually:

- review the length of time we keep personal data;
- consider the purpose or purposes that we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date or is no longer required.

Who we share this information with

Your information will be shared internally, including with members of the HR team, the finance department, your line manager and IT staff if access to the data is necessary for performance of their roles. Should a grievance or disciplinary investigation be required, relevant information to that investigation may be shared upon approval by the Executive Director of People and Purpose.

The College shares your data with third parties as below:

- In order to obtain references from other employers and obtain necessary criminal records checks from the Disclosure and Barring Service
- Pension providers and Payroll providers (where a third party is used)
- HM Revenue and Customs
- Police and Enforcement Agencies, and emergency services in the event of an emergency
- Information Commissioner's Office (ICO) (complaints/breaches investigations)
- Where necessary or mandatory, we will disclose personal information in connection with investigations, disputes, complaints and grievances internally and with third parties for example local authority safeguarding boards, trade unions, government departments and agencies, insurers and legal representatives and professional bodies to which a member of staff is affiliated e.g. CIMA, CIPD
- Recruitment and employment agencies
- Previous and future employers/referees – pre and post contract and governor checks
- External Training/Travel Providers – booking and administration purposes
- Government departments including: Department for Education (DFE) (www.gov.uk/df), Office for Standards in Education, Children's Services and Skills (www.gov.uk/ofsted), Office for National Statistics (www.ons.gov.uk), Education Skills and Funding Agency (www.gov.uk/esfa)
- Personal information relating to any person(s) involved in administering, teaching or completing examinations/assessments where malpractice is suspected or alleged may be shared with other awarding/validating bodies, the qualifications regulator or other professional bodies and where relevant in accordance with the JCQ publication Suspected Malpractice in Examinations and Assessments – Policies and Procedures.
- Awarding/validating bodies for general administration, quality control and queries
- The College also shares your data with third parties that process data on its behalf, in connection with payroll, pension scheme providers, the provision of benefits and the provision of occupational health services.
- The College may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

We will only share your information with partners or suppliers who have sufficient measures and procedures in place to protect your information and can meet their legal obligations under data protection legislation.

We may also be required to share information in connection with DSAR requests (Data Subject or Authorised Representative) e.g. information which may be contained within emails, documents, systems, paper and electronic records/filing systems and other forms of media, this may include work email address(es), work contact details and also the disclosure of information of which you were the author or to which you have contributed. This includes deleted and archived personal

information which is still accessible.

Why we share 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.

Data Collection & Processing for Applicants:

How we use your information

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for.

Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.

Candidates are asked to provide proof of identity and qualifications at the interview. Photocopies of original documents are only retained if the candidate is successful.

If you are unsuccessful for the position you have applied for, your data will be held for a period of six months in case of any queries regarding the outcome or for feedback purposes.

Conditional offer

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and assess suitability for the role.

Upon commencement of your employment, we will also ask you for:

Bank details – to process salary payments

Emergency contact details – so we know who to contact in case you have an emergency at work

Employment status for tax code purposes.

Our contract of employment requires all staff to declare if they have any potential conflicts of interest, other employment or engagement. If you complete a declaration, the information will be held on your personnel file.

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 Oliver Roth, Data Protection Officer.

You also have the right to:

- the right to be informed about the collection and use of your personal data
- access and obtain a copy of your data on request;
- require the College to change incorrect or incomplete data;
- require the College to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- obtain and reuse your personal data for your own purposes
- object to the processing of your data where the College is relying on its legitimate interests as the legal ground for processing; and
- ask the College to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the College's legitimate grounds for processing data or 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 ask that you raise your concern with us in the first instance. 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: Oliver Roth, Executive Director MIS and Digital Transformation & Data Protection Officer, oroth@buckscollegigroup.ac.uk.