Privacy Notice – Staff

Bridgwater & Taunton College is committed to the data security and the fair and transparent processing of personal data. This privacy notice for staff sets out how we will treat your personal data which you provide us in compliance with the UK General Data Protection Regulation (UK GDPR).

We are the data controller of the personal information about you. We are: Bridgwater & Taunton College. Our address is: Bath Road, Bridgwater, Somerset TA6 4PZ and is registered with the Information Commissions Office (ICO), Registration Number Z4677243.

Our Data Protection Officer is Emma Kilner. If you have any questions about this policy or the ways in which we use your personal information, please contact our Data Protection Officer

Personal data we hold on you

The types of data we hold and process will typically include:

Personal information

- Contact details, including title, full name, address, telephone numbers and email addresses
- Identifying details, including date of birth, national insurance (NI) number and photographs
- Information relating to your employment, both current and historical, including length of service, contract details, salary, performance, appraisal, disciplinary and grievance
- Official documentation for confirming your personal identify, address and right to work in the UK/immigration status (e.g., passport, driving license, birth/adoption certificate, marriage certificate, divorce documentation, qualification certificates, bills/government letters)
- Other information in relation to your terms and conditions of employment including benefit memberships (including but not limited to pension, golf course, gym) to enable the calculation, deduction, or payment of benefits, for example bank account details.
- Information about your family, dependents, or personal circumstances, for example marital status, childbirth and leave (maternity/adoption or paternity/parental leave) for statutory and contractual pay/leave, jury service.

Special information

- Information about your health or disability information. This may include pre-employment occupational health (OH) information, in-employment health assessments or reviews (with an outsourced OH service or from your GP/Consultant) or other health professional.
- Information about any criminal convictions, declared at the time of your pre-employment checks or during your employment, which may include cautions, convictions, reprimands, warnings, or fines.
- Information about your race or ethnicity, religious beliefs and sexual orientation.

We will use your personal and sensitive data:

- to communicate with you about all aspects of your recruitment or employment;
- to employ you and support your attendance at work and to make reasonable adjustments to support the performance of your role;
- to process employment related changes and staff benefits (e.g. sick pay, pension membership)
- to process staff development and training booking requests
- to make travel arrangement bookings
- to operate effective and professional communication and security systems (e.g. email and staff identification/access badges) including the taking, storage and supply of your photograph
- to provide references to potential employers, voluntary organisations or for qualifications during or after your employment ends
- to request and process visa, immigration and certificate of sponsorships and liaise with the relevant Government Departments
- to process UK and public sector reporting obligations, (e.g. Gender Pay Gap, Equality Duty, government statistical returns).

How we collect and use your data

We obtain most of the personal and sensitive information directly from you.

We may also obtain data from third parties e.g. your previous employers in reference requests (for example, salary information, parental leave information and NI number or date of birth), HMRC, occupational health providers. We may also obtain special information from a Disclosure & Barring Service Certificate, completed as part of our safer recruitment and pre-employment verification processes.

Our lawful basis for using this data

The College processes data to ensure that we are complying with our legal obligations. For example, we are required to check an employee's entitlement to work in the UK, to deduct tax, to meet Keeping Children Safe in Education guidelines, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, we have a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation 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 Enhanced DBS checks to ensure Safeguarding requirements are met

- 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 (OH) 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
- 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 organisation 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.

Special information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow the organisation to operate check-off for union subscriptions.

Where the organisation processes other special categories of personal data, such as information about the protected characteristics, this is done for the purposes of equal opportunities monitoring and related reporting activities such as our Equality Duties and Gender Pay Reporting.

The legal basis for our use of your personal data will generally be one or more of the following:

a) we need to process your personal data to satisfy our legal obligations as an employer
b) we need to process your personal data to carry out a task in the public interest or in the exercise of official authority in our capacity as a public body; and/or
c) we need to process your personal data for the legitimate interests of administering your employment, calculating and deducting pay related deductions (e.g. tax, national insurance or court orders), pension membership and other salary deductible memberships you may request from time to time.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated or new purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we will, if necessary, process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Failure to provider personal information

If you fail to provide certain information when requested, we will not be able to fully perform the contract we have entered with you (such as paying you or providing a benefit), or we could be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Information about criminal convictions

We will only collect information about criminal convictions or allegations of criminal behaviour where it is appropriate given the nature of the role and where we are legally able to do so.

Where appropriate, we will collect information about criminal convictions/allegations as part of the recruitment process or if we are notified of such information directly by you or a third party in the course of you working for us.

We will use information about criminal convictions/allegations and offences in the following ways to cross-refer to relevant policies/processes/vetting procedures, where we need to carry out our legal obligations or exercise our employment-related legal rights; and/or where it is substantially in the public interest to do so and necessary for performing our functions as a Public Body.

How we store and how long we keep your personal information

We will only keep your personal and sensitive data for as long as we need it to administer your employment and to deal with any questions or complaints that we may receive about this, unless the law requires us to keep it for a longer period.

In practice, this means that your personal and sensitive data may be retained for the duration of your employment and a period of up to 6 calendar years after you leave College employment.

There may be some pieces of information about you that are retained for longer than this period, and this is set out in legislation related to health and safety and statutory payments.

Types of Data	Retention Periods	Reason
Staff files including training records, medical information, records of disciplinary and grievance proceedings	6 calendar years from end of employment	References and potential litigation
Application forms and interview notes for unsuccessful candidates	6 months	Provide feedback to unsuccessful candidates, respond to claims

Your duty to inform us of changes

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

How we share your personal data

From time to time, we will share your personal data with third parties, including our contractors, advisors, government bodies and dispute resolution, law enforcement agencies and insurers

in order to comply with our obligations under law, and in connection with our employment obligations.

In some cases, these recipients may be outside the UK. If this occurs, we will make sure that appropriate safeguards are in place to protect your data in accordance with applicable laws. Please use the contact details below if you want more information in connection with this.

Rights of access, correction, erasure, and restriction

The details of your rights of access, correction, erasure and restriction are set out in the College's Data Protection Policy. For more information on how to make a request, please contact the Data Protection Officer by emailing dpo@btc.ac.uk

Concerns

We take your concerns and any complaints about the collection and use of your personal information very seriously. If you wish to query anything within this privacy notice, or think that your collection or use of personal data is unfair, misleading or inappropriate, please raise this with us in the first instance by emailing dpo@btc.ac.uk. Alternatively, you can make a complaint to the Information Commissioner's Office online at www.ico.org.uk/concerns or call 0303 123 1113.