BSU EMPLOYEES, APPLICANTS AND CONTRACTORS DATA PRIVACY STATEMENT

BUCKS STUDENTS' UNION

Updated: December 2023

BUCKS STUDENTS' UNION POLICY DOCUMENT

Introduction

Bucks Students' Union ("we", "our" or "us") promises to respect any personal data you share with us, or that we get from other organisations and keep it safe. We aim to be clear when we collect your data and not to do anything you wouldn't reasonably expect from us.

We are committed to protecting the privacy and security of your personal information. During the course of our activities, we will process personal data, which may be held on paper, electronic, or otherwise, about our staff and recognise the need to treat it in an appropriate and lawful manner, in accordance with the UK General Data Protection Regulation (UK GDPR). The purpose of this statement is to make you aware of how we will handle your personal data and applies to all employees, applicants and contractors. This privacy statement applies to all persons who provide HR and payroll information to the Union, regardless of their employment status.

Bucks Students' Union is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. Under data protection legislation, we are required to notify you of the information contained in this privacy statement. The statement applies to current and former employees, those applying to work with us and contractors. This notice does not form part of any contract of employment or other contract to provide services and we may amend it at any time.

It is important that you read this statement, together with other privacy statements that may be relevant to specific occasions, so that you are aware of how and why we are using such information. Additionally, this statement outlines what personal information is processed by the Union, the legal basis for processing personal data, storage and retention requirements, and the data subject's rights regarding their data.

Facilitating our legal requirements, organisation policy and services to our employees, through using your personal data, allows us to make better decisions, communicate more efficiently and, ultimately, ensure you receive the services required as a Union employee.

Data protection principles

We will comply with the six data protection principles in the UK GDPR, which say that personal data must be:

1. Processed fairly and lawfully.
2. Collected for specified, explicit and legitimate purposes and processed in an appropriate way.
3. Adequate, relevant and not excessive for the purpose.
4. Accurate and kept up to date.
5. Not kept longer than necessary for the purpose.
6. Processed in a manner that ensures appropriate security of the data.

"Personal data" means recorded information we hold about you from which you can be identified. It may include contact details, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you. "Processing" means doing anything with the data, such as storing, accessing, disclosing, destroying or using the data in any way.

Fair and lawful processing

We will usually only process your personal data where the processing is necessary to comply with our legal obligations, for the protection of your vital interests, for our legitimate interests or the legitimate interests of others. The full list of conditions is set out in the UK GDPR.

We will only process "special categories of data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, genetic data and data about sexual orientation where a further condition is also met. Usually this will mean that you have given your explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the UK GDPR.

What personal data we collect and how collect it

We may collect, store and use the following personal information about you:

- personal contact details, such as name, title, addresses, telephone numbers and personal email addresses
- date of birth
- gender
- student ID number, name of academic tutor, name of course and expected graduation date, if you are applying for a student role or opportunity
- marital status and dependents
- next of kin and emergency contact information
- details or qualifications and results
- National Insurance number
- bank account details, payroll records and tax status information
- salary, annual leave, pension and benefits information
- start date
- location of employment of workplace
- copy of driving licence, if applicable (e.g., minibus driver)
- recruitment information (including copies of right to work documentation, references and other information included in a CV, cover letter or as part of the application process)
- employment records (including job titles, work history, working hours, training records and professional memberships)
- performance information
- disciplinary and grievance information
- CCTV footage and other information obtained through electronic means
- information about your use of our information and communication systems
- photographs
- relationship status with any Students' Union or University staff
- contact details of references.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- information about your health, including any medical condition, health and sickness records
- information about criminal convictions and offences.

How we collect your personal information

We typically collect personal information about employees, applicants and contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties, including former employers, credit reference agencies or other background check agencies.

We will collect personal information in the course of job-related activities throughout the period of you working for us.

How we will use your personal information

We will only use your personal information when the law allows us to. We will process data about staff for legal, personnel, administrative and management purposes and will use your personal information in the following circumstances:

- where we need to perform the contract we have entered into with you
- where we need to comply with a legal obligation
- where it is necessary for our legitimate interests, or those of a third party, and your interests and fundamental rights do not override those interests

We may process special categories of data relating to staff, including (as appropriate):

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work
- the employee's gender, sexual orientation, racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
- in order to comply with legal requirements and obligations to third parties.

Situations in which we will use your personal information

We need the information that you provide to us, as detailed above, primarily to perform our contract with you and enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. More specifically, the situations in which we will process your personal information are listed below:

- making a decision about your recruitment or appointment
- administering the contract we have entered into with you
- determining the terms on which you work for us
- checking you are legally entitled to work in the UK
- paying you and deducting tax and National Insurance contributions
- providing you with additional benefits, for instance: pension, flu jabs (on request), training and development

opportunities, free attendance at our events, etc

- liaising with your pension provider
- business management and planning, including accounting and auditing
- conducting performance reviews, managing performance and determining performance requirements
- making decisions about salary reviews and compensation
- accessing qualifications for a particular job or task, including decisions about promotions
- gathering evidence for possible grievance or disciplinary hearings
- making decisions about your continued employment or engagement
- making arrangements for the termination of our working relationship with you
- education, training and development requirements
- dealing with customers and other third parties to whom your identity and background information is important
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- ascertaining your fitness to work
- managing sickness absence
- complying with health and safety obligations
- to prevent fraud
- to monitor your use of our information and communication systems to ensure compliance with both the Union and University's IT policies
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- to conduct data analysis insights to review and better understand employee behaviour, satisfaction and retention
- equality, diversity and inclusion monitoring
- to undertake criminal background checks, through the Disclosure and Barring Service (DBS), for certain positions, for instance welfare roles and minibus drivers.

Some of the above grounds for processing might overlap and there may be several groups which justify our use of your personal information.

If you do not provide personal information

If you fail to provide certain information when we requested, we may not be able to perform the contract we have entered into with you, such as paying you or providing you with a benefit. We may also be prevented from complying with our legal obligations, such as ensuring the health and safety of our team.

Change of purpose

We will only process your personal data for the specific purpose or purposes notified to you or for any other purpose specifically permitted by the UK GDPR. The data will only be processed to the extent that it is necessary for the specific purposes notified to you. If we need to use your personal information for an unrelated purpose, we will notify you and explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules and where this is required or permitted by law.

How we use particularly sensitive personal information

Special categories of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our privacy standard.
3. Where it is needed in the public interest, such as for equality, diversity and inclusion monitoring or in relation to our pension scheme and in line with our privacy standard.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims, or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use particularly sensitive personal information:

- relating to leaves of absence, which may include sickness absence or family-related leave, to comply with employment and other laws
- about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits
- about your race or ethnical origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equality, diversity and inclusion monitoring and reporting.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This is usually where such processing is necessary to carry out our obligations and provided we do so in line with our privacy standard. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made this information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so (for instance, but not limited to, certain welfare roles and drivers of the night-time SSHH bus). We envisage that we hold this information about criminal convictions. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or where we need that information because of your role. For certain roles, we may undertake a criminal background check, through the Disclosure and Baring Service. We may be notified of such information directly by you in the course of you working for us. We are allowed to use your personal information in this way to carry out our obligations.

Data sharing

We may have to share your data with third parties, including our members, third-party service providers and other people, businesses or organisations. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside of the UK/EU for any of the purposes described in this statement. Where we do so, you can expect a similar degree of protection in respect of your personal information.

Why we might share your personal information with third parties

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" include third-party service providers, including contractors and designated agents, and other entities. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, account systems and online banking. In addition, personal information may be also be shared with our employment lawyers, auditors and financial advisors and, in certain circumstances, Buckinghamshire New University.

How secure is my information with third-party service providers?

All of our third-party service providers and other entities are required to take appropriate security measures to protect your personal information under the general law or in line with any agreements. We do now allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Transferring information outside the UK and EU

We may transfer the personal information we collect about you to countries outside the UK in order to perform our contract with you. There may not be an adequacy decision by the UK courts or legal system in respect to those countries. This means that the countries to which we transfer your data may not be deemed to provide an adequate level of protection for your personal information. However, to ensure that your personal information does receive an adequate level of protection, we have put in place appropriate measures to ensure that those third parties are treating the information in a way that is consistent with and which respects the UK GDPR and laws on data protection:

- all third-party sharing to be undertaken with a valid contract only
- all third parties to be auditable by the Data Protection Officer for BSU

If you require more information about these protective measures, you can speak to the Data Protection Officer.

Data retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employer or contractor of the organisation, we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

How secure is my data?

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. We have put in place procedures and technologies to safeguard and maintain the security of all personal data from the point of collection through to destruction. Maintaining data security means guaranteeing the confidentiality, integrity and availability of personal data. In addition, we undertake regular reviews of who has access to information that we hold to ensure that your information is only accessibly by appropriately trained staff and contractors.

We provide a Data Protection and Information Security Policy which is supported by a practical handbook for our employees and volunteers. As an employee or contractor, you will be required to undertake general data protection training that is provided through the University.

Right of access, correction, erasure and restriction

Your duty to inform us of changes

We will keep the personal information we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. Please keep us informed if any of your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

Processing in line with your rights

You have the right to:

- request access to your personal information. This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it

- request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us to continue processing it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing
- object to processing of your personal information where we are relying on a legitimate interest (or those of a third-party) and there is something about your situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- request the restriction of processing your personal information. This enables you to ask us to suspend the processing of personal information about you. For example, if you want us to establish its accuracy or the reason for processing it
- object to processing that is likely to cause unwarranted substantial damage or distress to you or anyone else
- object to any decision that significantly affects you being taken solely by a computer or other automated process.

If you want to review, verify, correct or request erasure of your personal information, or object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Data Protection Officer in writing.

Requesting access to your information

If you wish to know what personal data we hold about you, you must make the request in writing. All such written requests must be forwarded on to the Data Protection Officer. There will be no fee charged to access your personal information or to exercise any of the other rights. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances. At the point of making a request, we may need to request specific information from you to help us confirm your identity. This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Breaches of data protection principles

If you consider that the data protection principles have not been followed in respect of personal data about yourself, or others, you should raise the matter with your line manager, in the first instance, and then the Data Protection Officer. Any breach of the UK GDPR will be taken seriously and may result in disciplinary action.

Data Protection Officer

We have an appointed Data Protection Officer (DPO) to oversee the compliance with this privacy statement, other privacy statements and general operational aspects of data. If you have any questions about this privacy statement, please contact the Data Protection Officer. You also have the right to complain to the supervisory authority, and, in the UK, that is the Information Commissioner's Office (ICO). More details on how to complain are available on the ICO's website at www.ico.org.uk/make-a-complaint.

Changes to this statement

We may change this privacy statement from time to time. If we make any significant changes in the way we treat your personal information then we will make this clear on our website or by contacting you directly.

If you have any questions, comments or suggestions, please let us know by contacting sudataprotection@bucks.ac.uk.