

Employee Data Privacy Statement

Introduction

University of Brighton Students' Union ("we", "our" or "us") promises to respect any personal data you share with us, or that we obtain from other organisations, and to keep it safe. We are committed to protecting the privacy and security of your personal information and aim to be clear when we collect your data and not do anything you wouldn't reasonably expect.

University of Brighton Students' Union is a "data controller" which means that we are responsible for deciding how we hold and use personal information about you. This privacy statement outlines how we collect and use personal information about you before, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

This notice applies to candidates, current and former employees, workers and contractors. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

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

What is personal data?

Personal data is any information that tells us something about you. This could include information such as your name, contact details, date of birth, and references.

How do we collect information about you?

When you apply for a role

When you apply for a role at Brighton Students' Union, you will normally apply direct and complete an Application Form. Alternatively, you might apply through an Agency who will send us a copy of your CV. The Application Form or CV will collect personal information from you. The Union has a legitimate interest in processing this data for the purposes of considering you for that role and for anonymous statistical analysis.

Some special categories of sensitive data will be collected through an Equal Opportunities Form but completion of the form is voluntary and is for statistical analysis only. The legal basis for the Union having this personal data is consent and the information provided will be kept strictly confidential and stored securely within the HR Department.

When you become an employee

When you become an employee of the Students' Union, you form a contract with us which declares that we will process some personal and sensitive data to comply with our legal obligations and to fulfil our policies and procedures.

When a third-party provides us with your data

Your information may be shared with us by independent organisations such as Her Majesty's Revenue and Customs (HMRC), Child Support Agency, Student Loans Company, court rulings or external references.

These independent third-parties will only do so when you have indicated that you have given consent or there is a legal obligation to share this data with us. You should check their privacy policies when you provide your information to understand fully how they will process your data.

What information do we collect and how do we use it?

The type of information we collect and how we use it depends on why you are providing it.

From candidates

If you are applying for a role with us we collect, or may collect, the following categories of information about you:

- Personal contact details such as name, title, address, telephone number and personal email addresses
- Employment and volunteering history
- Equal opportunities information such as age range, gender, race, ethnicity, religion, health & sexual orientation
- Recruitment information (including copies of right to work documentation, references and other information detailed on documentation provided as part of the application process)
- Information about criminal convictions and offences committed by you

If you are applying for a Student role or opportunity we will also ask you for:

- Student ID number
- Name of academic tutor
- Name of course and expected graduation date

We will mainly use your data to communicate with you and:

- Make decisions about your recruitment and appointment
- Check you are legally entitled to work in the UK
- Assess your qualifications for a particular job or task
- Conduct data analytics studies to review and better understand job application rates
- Carry out equal opportunities monitoring

From employees

When you commence employment with Brighton Students' Union, in addition to the data provided during the recruitment process, we will ask you to provide:

- Bank account details
- Emergency contact details
- Identity and address verification documentation
- Earnings deductions including student loans, etc

During the course of your employment, the Students' Union may collect the following data:

- Health records, physician details and sickness absence data
- Performance and development records and communications

We will mainly use your data:

- For administrative functions relating to your employment, including the payment of salaries
- To fulfil our obligation as your employer under the terms and conditions of employment as agreed by you
- To manage sickness, wellbeing and workplace performance

Contractors

Depending upon the nature of the contractor's recruitment, role and payment method within the Union, they may be asked to supply some or all of the above information relating to applicants and employees.

What happens if you do not provide information that we request?

We need some of your personal data in order to conduct the recruitment and selection process and administer the employment contract. If you do not provide such information, we may not be able to continue with the recruitment process or your continued employment with us may be put at risk. In this situation we would explain the reasons at the point where we collect the information from you.

How do we use your information?

Under data protection legislation we are only permitted to use your personal data if we have a legal basis for doing so as set out in the data protection legislation. We rely on the following legal bases to use your information for employment/engagement related purposes:

- Where we need information to enter into a contract 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

What is Sensitive Data?

Some information is classified as "special" data under data protection legislation. This includes information relating to health, racial or ethnic origin, religious beliefs or political opinions, sexual orientation and trade union membership. This information is more sensitive and we need to have further justifications for collecting, storing and using this type of personal data. Eg processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

There are also additional restrictions on the circumstances in which we are permitted to collect and use criminal conviction data. We may process special categories of personal data and criminal conviction information in limited circumstances with your explicit consent, in which case we will explain the purpose for which the information will be used at the point where we ask for your consent.

How do we share your information?

We share your personal data in the following ways:

- Where we use third party services providers who process personal data on our behalf in order to provide services to us. This includes Recruitment Agencies, IT and benefit providers

- We will share your personal data with third parties where we are required to do so by law or to comply with our regulatory obligations
- With other entities in our group as part of our regular reporting activities and in the context of a business reorganisation or group restructuring exercise
- If we sell any part of our business and/or integrate it with another organisation your details may be disclosed to our advisers and to prospective purchasers or joint venture partners and their advisers

Where we share your personal data with third parties we ensure that we have appropriate measures in place to safeguard your personal data and to ensure that it is solely used for legitimate purposes in line with this privacy notice.

The Union do not sell any personal data related to our candidates or employees or transfer data to any third party, unless there is a legal requirement to do so. We may need to disclose your details to the police, regulatory bodies or legal advisors if required. We will only ever share your data in other circumstances if we have your explicit and informed consent to do so.

How do we keep your information secure?

Your employment related data may be stored in any of the following:

- Secure storage on network drives. These are shared computer drives hosted by the University of Brighton who have appropriate firewalls in place. Access to the drives are password protected and limited to the team of staff who may process the data.
- Folders are kept within a locked filing cabinet within the HR office. Access to the offices is restricted to a limited number of employees, and access to the filing cabinet is restricted solely to those that may process the information.
- Some information may be shared via email, this is only done via the secure outlook 365 system which is password protected and has suitable firewalls in place. Passwords are applied to certain files when sharing via email.
- Data is stored within the BreatheHR system. This data and the company's use of it is compliant with the GDPR regulations and there are extensive protection systems in place to ensure its security. Detailed information regarding this can be found on the company's website via <https://www.breathehr.com/hr-software/security-reliability>.
- Very occasionally, when other options are not suitable, a portable storage device such as a memory stick might be used. In these circumstances, the device would be encrypted with password protection, and only used for the period of time required.
- Limited elements of your data might be stored in other systems, which you have access to or are required to use. For example, your name and basic details might be held in the system which manages access control for the building.

We will ensure access to personal data is restricted to employees working within our group on a need to know basis. Training will be provided to any employees working within the group who need access to your personal data to ensure it is secured at all times. Suitable procedures are in place to ensure information is only kept as long as it is required, after which it is destroyed in a secure fashion.

When do we transfer your information overseas?

Brighton Students' Union does not currently send or store personal data outside of the European Union and it is most unlikely that we would need to transfer such information abroad.

However, when data is transferred to countries outside of the UK and the European Economic Area those countries may not offer an equivalent level of protection for personal data to the laws in the UK. Where this is the case we would ensure that appropriate safeguards were put in place to protect your personal data. It's possible that a data transfer or storage method such as drobox could be used, which may mean in these circumstances, that the information would be stored within the United States. Due diligence would be taken before using a method within the United States. If the need arose, we would seek your permission before doing so.

For how long do we keep your information?

Candidates

As a general rule we may keep personal data about candidates for the duration of the recruitment and selection process and for a period of 12 months after candidates have been notified whether their application has been successful. However, where we have statutory obligations to keep personal data for a longer period or where we may need your information for a longer period in case of a legal claim, then the retention period may be longer.

Employees

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 employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

Keeping your information up-to-date

It is the responsibility of individuals to ensure that their personal information is kept up to date at all times whether this is during the recruitment process or during employment with us. For employees, this must be done using the agreed procedures in place – eg via BreatheHR for established staff and Staff Savvy for student staff.

Your rights in relation to your information

You have a number of rights in relation to your personal data, these include the right to:

- Be informed about how we use your personal data
- Obtain access to your personal data that we hold
- Request that your personal data is corrected if you believe it is incorrect, incomplete or inaccurate
- Request that we erase your personal data
- Ask us to restrict our data processing activities
- Request a copy of certain personal data
- Object to our processing of your personal data
- Not be subject to automated decisions

How can I raise a query, concern or complaint?

Brighton Student Union have appointed the Chief Executive Officer as a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you would like to exercise any of your rights, have any questions about this document or the way in which we handle your personal information, please contact the DPO:-

Name Laura Greenwood-Pearsons
 Address Data Protection Officer
 Brighton Students' Union
 Watts Building
 Lewes Road
 Brighton
 BN2 4GJ
 Email Address l.greenwood-pearsons@brighton.ac.uk
 Telephone Number 01273 642872

If you remain dissatisfied then you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Address Information Commissioner's Office
 Wycliffe House
 Water Lane
 Wilmslow
 Cheshire
 SK9 5AF
 Website Address www.ico.org.uk

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.

EMPLOYEE SIGNATURE			
I confirm that I have received a copy of the University of Brighton Students' Union Employee Data Privacy Statement and that I have read, understood and accept it.			
Employee Name		Job Title	
Signature		Date	