

## Privacy Statement – UUSU Advice Bureau

### 1. Introduction

The UUSU Advice Bureau (us, we, our) takes your data protection and rights in relation to this very seriously. We have written this document to make things as clear as we can, if you have any questions about your privacy in relation to getting support from the Advice Bureau then please contact us (details in section 10). For the avoidance of doubt support can mean: representation, information, advice etc. and should be read as such through the rest of this document.

We promise to respect and protect any data you share with us; we won't do anything with your data that you wouldn't reasonably expect us to do when you contact us for support.

Data protection in the UK is overseen by the Information Commissioner's Office (ICO) and the main legislation that underpins it is derived from the EU General Data Protection Regulations (2016) (GDPR). The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

### 2. What Data We Collect

When you contact us and ask for support we keep a record of the information you have provided and our response to you. This can range from one email to detailed notes on meetings that we have had with you – depending on the complexity and nature of your situation.

We may ask you to fill out a form when you approach us for support, this asks a range of demographic questions as well as your basic details. Some of this demographic data is considered special category data under the law. Because of this we need to get your direct consent to process this data. Processing data includes: collecting, recording and storing.

Special category data is anything related to the following:

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

There is more info on what consent means in section 5.

### 3. How We Collect and Use Your Data

The Advice Bureau is an independent and confidential service (see section 4 for more about what this means). We process your data for our own records, it is stored electronically in a secure environment and externally to the Union and the University servers. We will never use the information about you for marketing purposes.

We collect data about you in three ways, either directly from you, directly from a person/third party you have given consent to share information with us, or from your University Banner record. We have

a data sharing agreement with the University to access certain basic details about you on Banner. This includes your student number, name, term time address, student email, gender, whether you are a mature student, and course details. This has been set up so that we can ensure the best service support for you, and you don't need to go through it all directly with us. If you have any questions about this, please see section 10 on how to contact the University's Data Protection Officer.

We use your data for two purposes. The first and most important is to help you with your case/problem. We collect your data with your initial consent and then process it through legitimate interest, it is necessary for the Advice Bureau to protect your interests as our client as well as our interests as a service. We believe that you have a right to complain if the advice you receive is incorrect or unsatisfactory. Without storing data, including case details, it may be difficult for you to seek redress. We require your data in the event of a complaint so that we can check if the advice provided was accurate and you were treated in a fair and respectful manner.

The second reason that we process your data is for monitoring and statistical purposes. At this point any personal or identifiable data is anonymised. We then use this to look at trends/patterns so that we can focus our work on helping students in the most effective way. For example, if we see that a lot of mature students or students in a department are having the same problems we can look at ways to prevent these problems from occurring in the first place. An example of how we would do this, would be to approach the University about changing a policy or looking at how we can better provide support to a particular group of students with the anonymised data.

We also want to make sure that we are giving you the best support possible, so we regularly have monitoring reviews and audits of our service. This means that your case might be looked at by an external party (for example another Advice Service at another institution), but your identifying and personal data will be removed first.

#### 4. Sharing Your Data and Disclosure to Others

In general, we will not share your information outside of the Advice Bureau without your direct consent (see section 5 for more info on consent and what this means). However, there are some instances where we have a statutory obligation to share your data. These are instances that are set out in Acts of Parliament or by a Court of Law. They include criminal and terrorist activity, adult and child protection concerns, conflict of interest, or if we believe there is a substantial threat to life/harm of you or another person. You can read more details about this in our Confidentiality Policy.

#### 5. Consent

Consent has been clarified and defined in the GDPR. It must be a clear process and involve a positive choice from the person giving it (no pre-ticked boxes or opt out options are now allowed). You are also able to withdraw your consent at any time and we can't refuse to support you on that basis alone.

We will ask for your explicit consent for two reasons. The first is to process specially protected data about you (like if you have a disability or your sexual orientation), we use this data to inform our work and monitor our service (see section 3).

The second reason is to get your permission to share your information when it is relevant/necessary to support you. If we deem this necessary we will ask you to sign a mandate allowing us to share your information, this can only be to specific people for a specific purpose. For example, if you want representation in an academic discipline case you will need to give us your consent to speak with the University about your case.

## 6. How to Change and Erase Data We Hold on You

You have the right to be able to see the information we hold on you, have any incorrect facts changed and to have your data erased. If you want to exercise any of these rights, please contact us (see section 10) and we will talk you through the process.

## 7. Your Rights

The GDPR sets out your rights as an individual, we strive to uphold and protect your rights in balance with our legitimate interest in providing support for you.

You have:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

You can see detailed explanations on each of these rights [here](#).

## 8. Keeping Information Secure

We have explained why we process your data; we also want to explain the actions we take to keep it secure. We store all your data on a system called Advice Pro. This is held securely and externally to both the Union and the University and is only accessible to The Advice Bureau staff. Advice Pro advocates privacy by design and as such annually employ the NCC Group to undertake penetration testing, one of the top three companies providing the service. Advice Pro is a highly trusted case management system within the advice sector and is fully compliant with the GDPR. Their GDPR Factsheet provides an overview of how their functionality and design features for the system comply with GDPR: [here](#)

Any documentation not stored on Advice Pro will be kept in your Adviser's secure and encrypted personal drive or within a locked cabinet in a locked office.

## 9. Time Frames

The GDPR states that we can only keep your data for no longer than it would be reasonable for the purposes that we have outlined. We have considered this, and we feel that a six-year retention period gives you the opportunity to re-engage with our service throughout your time at University. This means that if an issue in your first year occurs again in final year we still have your details and you don't need to go through the same process twice. Some issues, like complaints, can still be in process after you have left the University, which is why we feel 6 years is an appropriate time scale. After this time all your data will be automatically archived from Advice Pro and any other internal systems (fully anonymised with all personal data erased and only accessible as a wider pool for anonymised data for statistical reporting).

## 10. How to Contact Us

If you have any questions about privacy and confidentiality, please get in touch:

The Advice Bureau, UUSU, [advice@uusu.org](mailto:advice@uusu.org)

Chief Executive Officer, UUSU and Data Protection Officer, David Longstaff [d.longstaff@uusu.org](mailto:d.longstaff@uusu.org)

Ulster University Data Protection Officer, Eamon Mullan, [e.mullan@ulster.ac.uk](mailto:e.mullan@ulster.ac.uk)