

## How the University uses student personal data (Fair processing notice) 2016/17

The University needs to process student personal data in order to function effectively as an educational institution and to provide students with the support they require while undertaking their studies. Personal data is processed for a variety of reasons (as set out below) and all such personal data shall be collected and held in accordance with the Data Protection Act 1998 ('the Act').

### Types of personal data processed

Personal data the University may process:

- personal details (name, address, date of birth)
- phone numbers
- email addresses
- gender
- gender identity
- photographs
- financial information
- academic marks
- appraisals
- references
- disciplinary information
- criminal offence or conviction information
- health and disability information
- ethnicity data
- sexual orientation
- dietary requirements
- religious belief data
- caring responsibilities
- information regarding hobbies and interests
- any other legitimate personal data relating to academic and pastoral support.

Information about criminal offences, health, disability, ethnicity, sexual life and religion constitutes sensitive personal data (as defined within [s.2 of the Act](#)) and is afforded an extra level of security and confidentiality.

Emergency contact details provided by students are held. Students should notify the relevant person that they are providing their contact details to the University as their listed emergency contact.

### Primary purposes for processing

- Student welfare / pastoral care – e.g. contact with personal tutor, Counselling Service
- Administration and provision of health care services - Student Health Service
- Financial administration – e.g. payment of tuition fees, provision of loans and bursaries via the Student Funding Office
- Security and crime prevention / detection – e.g. use of regulated CCTV, security incident reports
- Library services – e.g. administration of membership, cards, loans and fines

- Provision of student ID card
- Provision and maintenance of computing facilities - including email accounts and internet access
- Educational administration – e.g. registration, progress monitoring, timetabling, calculation and publication of assessments, provision of references
- Accommodation - provision and management of University owned and privately owned property for students
- Administration of applications - receiving and processing UCAS forms, compilation of statistics, assessments of applications including preliminary and confirmed offers. Some liaison with UCAS.
- Advisory services – e.g. careers and financial advice

This is not an exhaustive list but sets out the primary reasons the University handles student personal data.

The University will also use student personal data to produce non-identifiable statistical data for analysis to fulfil its commitment to equality monitoring and provide a more targeted response to improving the student experience.

### **Disclosures to third parties**

Where there is a legitimate or legal reason to do so, the University may disclose student personal data to the following third parties:

- [HESA](#)
- [Student Loans Company](#) (to allow students to receive their loans)
- Local Education Authorities
- Local authority (Bristol City Council) - in relation to Council Tax exemption, maintaining the electoral roll and administration of housing benefit
- UK Visas and Immigration ([information on immigration and visas](#))
- [General Medical Council \(GMC\)](#) - for medical graduates, to process and maintain registration with the GMC
- [General Dental Council \(GDC\)](#) - for dental graduates, to process and maintain registration with the GDC
- [The Students' Union](#) (Bristol SU) – the University will provide Bristol SU with student personal data to allow it to create and manage its membership list
- [JISC Plagiarism Detection Service](#) (Turnitin)
- External accommodation providers - where student accommodation is provided on behalf of the University
- Research councils
- Agents assisting the University with international admissions (this may include the disclosure of personal data outside the [European Economic Area](#))
- External auditors
- External examiners
- Other higher education institutions, partners or research organisations where a student's programme is being run collaboratively
- Third parties performing administrative functions on behalf of the University (acting as data processors)
- Police and other investigative agencies – only where the disclosure of personal data would assist with the investigation of a crime or other alleged misconduct. Such disclosures will be necessary and proportionate to the aims of the investigation

- Organisations seeking student views to enable the University to endeavour to improve the experience offered to students e.g. [National Student Survey](#)
- The Government and local authorities during information gathering exercises when the University is legally obliged to provide data
- Potential employers and other educational institutions requesting a reference for a current or past student (consent is implied by providing the University's details as a referee). This includes confirmation of awards.

This is not an exhaustive list and such third parties may have access to student data only for the purpose of performing their function. Any disclosures to third parties not listed here will be made only where there is a legitimate reason to do so and in accordance with the law.

The University may also use third party companies as [data processors](#) to carry out certain administrative functions on behalf of the University. If so, a written contract will be put in place to ensure that any personal data disclosed will be held in accordance with the Data Protection Act and have appropriate security measures in place.

Parents, family members and guardians are considered to be third parties and no student personal data will be disclosed unless consent is received from the student or the disclosure is otherwise in accordance with the Data Protection Act.

### **Collaborative programmes of doctoral training**

Please be aware that if you are applying for or enrolling on a collaborative programme of doctoral training (such as those listed on the [Bristol Doctoral College website](#)) then the University will need to make some further uses and disclosures of your personal data to administer your place on the programme. For further information, please see the relevant [Data Protection Statement](#).

### **Email**

Email for students is provided by a third party. This requires the University to disclose some personal data (name and email address) to this third party. This personal data will be held in accordance with the Data Protection Act and will be stored either in the EU or, if stored outside the EU, with a level of protection deemed adequate for the rights and freedoms of data subjects in relation to the processing of their personal data.

Students using the service are also subject to the third party's terms of use and privacy policy and are notified of these terms when issued with their account.

### **Student responsibilities**

Students processing personal data do not fall under the terms of the University's notification with the Information Commissioner's Office and must ensure that any personal data collected by in the course of their University work is held in accordance with the [Data Protection principles](#). Any research involving the use of personal data should only be conducted following an ethical review. Students are also subject to the [University's Information Security Policy](#).

Students also have a responsibility to ensure their personal details are up to date. This can be done online at [Student Info](#).

## **UCard (University ID card)**

The [UCard Privacy Policy](#) sets out how personal data, and other information related to the UCard, is handled.

## **CCTV**

The University operates CCTV around its properties for security and crime detection purposes. For further information, please see the University's [CCTV Code of Practice](#).

## **Accessing your personal data**

A [subject access request](#) may be made under the Data Protection Act to gain access to your personal data.

## **Retention**

Student files will normally be held for six years after a student has left the University. Basic information (including name, date of birth, attendance dates and award) about students will be retained indefinitely after a student has graduated or left the University.

## **Alumni**

On graduation, students will automatically become members of the University alumni and may receive information relating to alumni activities, such as news, events and fundraising opportunities. There is further information available about the benefits of being a Bristol alumnus on the [Campaigns and Alumni Relations Office website](#).

To opt out of receiving such information please send an email to: [alumni-change@bristol.ac.uk](mailto:alumni-change@bristol.ac.uk)

## **Further information**

The [Information Commissioner's Office](#) regulates the use of personal data in England and Wales.

For any queries regarding Data Protection, please contact the Information Governance Manager at: [data-protection@bristol.ac.uk](mailto:data-protection@bristol.ac.uk)