

HOW THE UNIVERSITY USES STUDENT PERSONAL DATA (FAIR PROCESSING NOTICE)

Introduction

Keele University collects, holds and processes personal data relating to its students, which is essential for it to manage its operations effectively. These activities are carried out in accordance with the Data Protection Act 1998 and the University's Data Protection Policy.

The data held by the University is mainly taken from the details students provide during the application and enrolment process and will be added to during and after the course of their studies.

During enrolment and subsequent annual re-enrolments, students give their consent for the University to process their personal data. The University provides this Fair Processing Notice to inform students of how their personal data will be processed and the purposes for which the data has been collected.

What is personal data?

The Act defines personal data as:

“data which relates to a living individual who can be identified from those data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller”.

In this case, the data controller is the University. It includes any expression of opinion about the individual as well as statements of fact.

What is meant by ‘processed’?

The processing of data includes obtaining, recording, storing, organising, maintaining, updating, retrieving, using, disclosing and deleting.

Types of personal data processed

Types of personal data the University may process, although not an exhaustive list, are:

- personal details (name, address, date of birth)
- email addresses
- gender
- photographs
- financial information
- academic marks
- attendance records
- references
- disciplinary information

- CCTV footage
- caring responsibilities

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.

The Data Protection Act 1998

The Data Protection Act 1998 requires that the University processes personal data in accordance with eight principles, which state that personal data must be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to countries without adequate protection

How your personal data will be used within the University

The official purposes for which the University processes personal data are notified to the Information Commissioner on an annual basis and can be viewed on the [Office of the Information Commissioner's website](#), quoting Registration Number **Z5571818**.

To manage its operations effectively, provide services to students and meet certain legal requirements, the University will process and maintain the personal data of its students. This personal data may include data such as name, address, date of birth, programme studied, fee payments, information about examinations, assessments and results.

In addition to this, the University may process some sensitive personal data about students, such as details about health in order to provide care, and information concerning ethnicity, sexual orientation, gender identity, domicile and disability for planning and monitoring purposes. Also, for certain programmes of study, information about past criminal convictions will be processed.

Personal data will be used within the University to provide students with services, such as accommodation, the Library and computer facilities and support, such as welfare and study advice. Any personal data shared in these ways will not be excessive. For example, the accommodation office will need a student's name, address, phone number in order to process their accommodation requirements, but it does not need to see their academic results.

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.

Sharing your personal data (disclosures to third parties)

The University may disclose appropriate personal data, including sensitive personal data, to third parties where there is legitimate need or obligation during or after the course of your studies. Such disclosure is

subject to procedures to ensure the identity and legitimacy of such agencies. These third parties may include the following:

- Higher Education Statistical Agency (HESA) – further information on how student data is used by the agency is contained within the HESA Student Collection Notice, which can be found at: <https://www.hesa.ac.uk/about/regulation/data-protection/notices>
- Student Loans Company (to allow students to receive their loans)
- UK Visas and Immigration (for international students)
- Accrediting bodies e.g. General Medical Council, Solicitors Regulation Authority
- The Students' Unions (KeeleSU and KPA)
- JISC Plagiarism Detection Service (Turnitin)
- External email provider (name and email address)
- External accommodation providers - where student accommodation is provided on behalf of the University
- Research councils
- UCAS
- Agents assisting the University with international admissions (this may include the disclosure of personal data outside the European Economic Area)
- Internal and 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)
- 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 (e.g. in relation to Council Tax exemption and the electoral roll for students residing in halls of residence)
- Police, crime or taxation agencies regarding the detection or prevention of a crime
- Potential employers and other educational institutions requesting a reference or confirming the award of a current or past student either directly or via the Higher Education Degree Datacheck (HEDD). Consent is implied by providing the University's details as a referee.

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.

Parents and family members

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 in accordance with the

Data Protection Act. The same is applied for landlords, sponsoring employers or sponsoring governments.

Your rights

Students have certain rights and responsibilities regarding their personal data, including:

- To be informed what personal data about you the University holds and what they are used for
- To access this personal data
- To update the personal data the University holds
- To be informed how the University is complying with its obligations under the Act
- To complain to the University if you believe that the Data Protection Policy has not been followed.

Students have a responsibility to ensure that the personal information they provide to the University is accurate and up to date. Information can be updated online via eVision.

Students wishing to receive a copy of their own personal data can do so by making a subject access request. Further information can be found on the University's Data Protection webpages at: www.keele.ac.uk/dpa.

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. Further information can be found on the University's alumni website at: www.keele.ac.uk/alumni.

Further information

For any queries regarding Data Protection, please contact the University's Governance Team.

The Information Commissioner's Office: www.ico.org.uk.