Kingston University London

Data Protection Policy

1. Introduction

Kingston University must retain and process personal data about its staff, students and other stakeholders to deliver its educational objectives. It is also necessary to process personal data to meet the University's legal obligations. To do this the University must comply with the General Data Protection Regulation (the "GDPR") from 25 May 2018 and a new UK Data Protection Act.

The GDPR protects individuals (data subjects) with regards to the processing of personal data by:

- Establishing a set of principles that govern personal data processing;
- Requiring personal data to be processed lawfully and fairly with a clear legal basis;
- Conferring rights on individual data subjects;
- Giving supervisory authorities (the Information Commissioner in the UK) responsibility for monitoring and enforcing the legislation.

The definition of personal data includes any physical or electronic information relating to an identifiable person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Most Kingston University staff and students (which are broadly defined and include honorary and part-time staff, agents, volunteers, contractors and others acting on behalf of the University) will have some contact with personal data and it is therefore essential that you are aware of the main principles of GDPR.

In addition, GDPR makes provision for the handling of special category (sensitive) personal data. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, health, sex life or sexual orientation data. This type of data requires additional safeguards and legal bases for processing. Similarly, personal data relating to criminal convictions and offences should be handled with particular care.

2. Data Protection Principles

The GDPR has six principles relating to the processing of personal data, which require that personal data must be:

1. Processed lawfully, fairly and transparently;
2. Collected for a specified purpose;
3. Limited to what is necessary in relation to the purpose for processing;

4. Accurate and up-to-date;
5. Retained for no longer than is necessary;
6. Processed in a manner that ensures appropriate security.

In addition, organisations have an accountability requirement to demonstrate their compliance with the principles. This means keeping accurate records about the personal data that the University processes, the reasons for the processing, who it is shared with and how long it is kept.

3. Status of this policy

This policy does not form part of the formal contract of employment for staff, or the formal offer of a place for study for students, but it is a condition of employment or study that employees and students will abide by the rules and policies made by the University from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

This policy should be read in conjunction with other relevant University policies and documents including the:

- Retention Policy;
- Retention Schedule;
- Data Protection Privacy Notices;
- Data Quality Policy;
- Freedom of Information Policy;
- IT Security Policy;
- Information Security Policy.

Collectively these documents set out the information governance framework within which all personal data within the University must be handled. They can be viewed on the University website.

4. Your responsibilities

When considering your own personal data, staff and students should ensure that the information that they have provided to the University remains accurate and up-to-date. You should inform the University as soon as possible if details, such as your address, change (this is a requirement of the Student Regulations).

When handling other people's personal data, staff and students are required to maintain confidentiality and abide by the GDPR principles. In particular you should ensure that:

- Personal data is stored securely;
- Procedures for handling personal data are documented and staff and students are made aware of these documents, their responsibilities and that they have appropriate training;
- Access to personal data should be restricted to those who need it for clearly defined purposes;

- Personal data is only collected and processed for a specific reason and must not be used for other unrelated purposes unless these were made known to the data subject or that additional permission has been obtained for further processing;
- Only the minimum amount of personal data necessary for the task is processed;
- Personal data is only retained for as long as it is needed for the original purpose and is not kept just in case it might one day be useful. Where a requirement is identified for long term retention, methods such as anonymisation should be considered;
- Particular care is taken when responding to requests to disclose the personal information of any data subjects, these requests should be promptly reported to the University's Data Protection Officer;
- Personal data is not transferred outside of the EEA without appropriate permission, this is particularly important if you are using free or paid for cloud-based services where data may be stored in another country.

Any breaches of personal data to individuals within or outside the University must be immediately reported to the University's Data Protection Officer.

5. Notification

The University is required to inform data subjects of the ways in which it processes personal data and the types of data held. The primary way that the University does this is through privacy notices published on the University's website. If you are establishing a new work process, information technology system or research project involving personal data this must be notified to the University's Data Protection Officer and/or the relevant ethics committee for assessment before the process, system or collection of personal data commences.

6. Liability

There is an agreed disciplinary procedure which is used to deal with proven cases of incompetence or negligence. You should also be aware that certain data protection breaches may be criminal offences.

7. Rights

Under GDPR staff and students (and members of the public) have rights in relation to their personal data. These rights are not absolute and may vary depending on the legal basis under which the University processes the personal data. However, broadly speaking data subjects have a right to:

- Know what personal data the organisation holds about them and get access to it;
- Have all or some of the data deleted or rectified where it is inaccurate;
- Object or restrict processing of their personal data.

If staff or students receive a request for personal data they must act promptly to inform the University's Data Protection Officer because the GDPR imposes strict time limits for responding.

Where staff or students wish to make their own requests in relation to their personal data they should do so via the Subject Access Request Form online or by email or writing to the University's Data Protection Officer: DPO@kingston.ac.uk.

There is no charge for such requests, unless they are manifestly unfounded or excessive.

8. Further information

Staff can contact their local GDPR Champion for further information. Staff and students should also familiarise themselves with the additional information in support of this policy on the University's Information Regulations section of the University website. This includes links to the University policies, privacy notices and related guidance.

9. Enquiries and complaints

Any questions relating to the GDPR or how the University is processing personal data should be addressed to the University's Data Protection Officer by email: DPO@kingston.ac.uk or by post: Data Protection Officer, Vice Chancellor's Office, River House, 53–57 High Street, Kingston upon Thames, Surrey KT1 1LQ.

If you or another data subject are not satisfied with how the University is processing personal data, a complaint can be made to the Information Commissioner.

You can find out more about your rights under data protection legislation from the Information Commissioner's Office website.