Data Protection Policy

Contents

OVERVIEW AND PURPOSE

1. Kingston University recognises the value of the personal data that we process and the need to collect, use and dispose of it appropriately and securely. The University endeavours to comply with the relevant data protection legislation (General Data Protection Regulation (GDPR), Data Protection Act (DPA) 2018 and the Privacy and Electronic Communications Regulations (PECR) and aims to inform, as transparently as possible, people (data subjects) about the purposes for which their personal data may be processed.

2. Data protection legislation protects 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 the Information Commissioner's Office responsibility for enforcement.

3. 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, a factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. In addition, the legislation 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.

4. Most Kingston University staff, students and other representatives will have some contact with personal data, and it is therefore essential that they are aware of the main principles of data protection legislation.

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

    - Processed lawfully, fairly and transparently
    - Collected for a specified purpose
    - Limited to what is necessary in relation to the purpose for processing
    - Accurate and up to date
    - Retained for no longer than is necessary

- Processed in a manner that ensures appropriate security.

6. Organisations also have an accountability requirement to demonstrate their compliance with the principles. This means keeping accurate records about personal data being processed, the reasons for the processing, who it is shared with and how long it is kept.

SCOPE

7. This policy applies to all staff, students and affiliates.

8. This policy applies to all personal data processed by or on behalf of the University.

POLICY

YOUR RESPONSIBILITIES

9. Staff, students and affiliates should ensure that the personal data they have provided to the University remains up to date. They should inform the University as soon as possible if details, such as their address, change (this is a requirement of the Student Regulations).

10. When handling other people's personal data, staff, students and affiliates are required to maintain confidentiality and abide by the data protection principles to 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 is restricted to those who need it for defined purposes
- Personal data is only collected and processed for a specific reason and must not be used for unrelated purposes unless these were made known to the data subject or that 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 personal data, these requests should be promptly reported to a line manager or the Data Protection team at datasubjectrequests@kingston.ac.uk

- Personal data is not transferred outside of the EU/EEA without appropriate permission and safeguards being put in place, 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 within or outside the University must be immediately reported to the University's Data Protection Officer at dpo@kingston.ac.uk.

NOTIFICATION

11. The University is required to inform data subjects of the ways 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 process, information technology system or project involving personal data this must be notified to the University's Data Protection Officer and/or the relevant ethics committee before the process, system or collection of personal data commences.

RIGHTS

12. Staff, students and affiliates (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 to or restrict processing of their personal data.

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

14. Where staff, students or affiliates wish to make requests in relation to their personal data they should do so via the Data Subject Request Form on the University's website or by email to the University's Data Protection team at datasubjectrequests@kingston.ac.uk. There is no charge for such requests unless they are manifestly unfounded or excessive.

ENQUIRIES AND COMPLAINTS

15. Any questions or complaints relating to data protection or how the University is processing personal data should be addressed to the University's Data Protection Officer by email at DPO@kingston.ac.uk or by post to Data Protection Officer, GCLO, Holmwood House, Grove Crescent, Kingston upon Thames KT1 2EE. If you 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.

RELATED LEGISLATION, REGULATIONS AND POLICIES

16. Related legislation

- UK Data Protection Act 2018
- UK General Data Protection Regulation

17. This policy should be read in conjunction with other relevant University policies and documents which can be viewed in the Information regulations section of the University website.

BREACH OF POLICY

18. Anybody handling personal data agrees to abide by the terms of any applicable policies. Users who are found to have breached the terms of relevant policies may be subject to warnings, verbal and written. In serious cases individuals will be subject to the University's disciplinary procedures, and possible legal action.