

KUSCO Data Protection Policy

What this policy covers

This Data Protection Policy relates to Kingston University Service Company Limited (hereafter KUSCO). KUSCO is a specialist service and facilities management company working exclusively for Kingston University.

The policy is applicable to KUSCO employees, contractors, suppliers and other stakeholders that process personal data on behalf of KUSCO. It details your rights and obligations in relation to the UK General Data Protection Regulation (GDPR) as amended by the Data Protection, Privacy and Electronic Communications Regulations, the Data Protection Act 2018 and the EU GDPR (hereafter the data protection legislation). It covers your own personal data and the personal data of third parties that you may come into contact with during the course of your association with KUSCO.

Definitions

For the purposes of this policy the following definitions apply:

- "Processing" is any use that is made of personal data, including collecting, storing, amending, disclosing or destroying it.
- "Personal data" is any information that relates to a living individual who can be identified from that information.
- "Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or political beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
- "Criminal offence data" means information about an individual's criminal convictions and offences and information relating to criminal allegations and proceedings.

If you have access to the personal data including special categories or criminal offence data of employees or of third parties, you must comply with this policy. Failure to comply with the policy and procedures may result in disciplinary action up to and including dismissal without notice.

Data protection principles

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 KUSCO processes, the reasons for the processing, who it is shared with and how long it is kept.

Your rights

Data protection legislation prescribes the way in which KUSCO may collect, retain and handle personal data. KUSCO will comply with the requirements of data protection legislation and all employees and others who handle personal data in the course of their association with KUSCO must also comply with it.

KUSCO will inform individuals of the reasons for processing their personal data, how it uses such data and the lawful basis for processing in the KUSCO Privacy Notice, which is available on the [website](#). It will not process personal data about individuals for other reasons.

Under data protection legislation you have the following rights:

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; and,
8. Rights in relation to automated decision making and profiling.

Please note that the above rights are not absolute, we may be entitled to refuse requests where exceptions apply. Further details about exercising data subject rights (including subject access requests) can be found below. Additional details on all of these rights can be found on the Information Commissioner's Office [website](#).

Your responsibilities

You are responsible for helping KUSCO keep your personal data accurate and up to date. You should let us know if your personal data changes, for example, if you change your bank or move to a new house.

You may have access to the personal data of other individuals and of our customers or clients in the course of your employment, contract, volunteer period, internship or apprenticeship. Where this is the case, KUSCO relies on you to help meet its data protection obligations.

If you have access to personal data, you are required:

- to access only data that you have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside KUSCO) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access including password protection, and secure file storage and destruction);
- not to remove personal data or devices containing or that can be used to access personal data, from KUSCO's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

Failure to observe these requirements may amount to a disciplinary offence, which will be dealt with under KUSCO's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee, customer or client data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to your dismissal without notice.

Data protection procedures

Processing special categories and criminal records data

Special categories data and criminal offence data require higher levels of protection. We need to have further justification for collecting, storing and processing these types of personal data.

KUSCO will process special categories and criminal offence data primarily where it is necessary to enable the company to meet its legal obligations. The full list of lawful bases for this processing is set out in the KUSCO Privacy Notice, which can be found on the [website](#) and in greater detail in the KUSCO Policy for Processing Special Category and Criminal Offence Data (KUSCO's 'appropriate policy document', which is available from HR upon request).

Accuracy and retention of personal data

KUSCO will review personal data regularly to ensure that it is accurate, relevant and up to date. The periods for which KUSCO holds personal data are contained in its Retention Schedule, which is available on the [website](#).

Security of personal data and data breaches

KUSCO will endeavour to ensure that personal data is not processed unlawfully, lost or damaged. If you have access to personal data, you must also comply with this obligation. If you believe you have lost any personal data, you must report it immediately. Failure to do so may result in disciplinary action up to and including dismissal without notice.

KUSCO will record all data breaches regardless of their effect. If we believe that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner's Office within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about the likely consequences of the breach and the mitigation measures we have taken.

All actual or suspected data breaches must be handled in line with KUSCO's Data Breach Policy and reported using the data breach form, which is available on the [website](#). You are responsible for ensuring that you have read and understood the Data Breach Policy.

Data subject rights (including subject access requests)

To exercise your rights, you should send your request to KUSCO. You can use the Data Subject Rights form available on our [website](#). Alternatively, you can contact our Data Protection Officer using the details at the end of this policy.

In most cases, KUSCO will need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

Under the data protection legislation, we are required to respond to a request within one month from the date we receive it. Where KUSCO requires proof of identity or clarification of the query the one-month time period will be put on hold. In some circumstances, for example where KUSCO processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell them if this is the case.

Where you request it, KUSCO will provide you with a copy of your personal data without charge unless the request is manifestly unfounded or excessive. This will normally be in electronic form if you have made the request electronically, unless you request otherwise. A request is likely to be manifestly unfounded or excessive where it repeats a request to which we have already responded. If you submit a request that is unfounded or excessive, we will notify you that this is the case and whether or not we will respond to it.

If you want additional copies, KUSCO may charge a fee, which will be based on the administrative cost of providing the additional copies.

Contact

If you have any queries or concerns about this policy please contact the KUSCO Data Protection Officer by email: KUSCODPO@kingston.ac.uk or by post: Data Protection Officer, KUSCO, Services Building, Penrhyn Road, Kingston upon Thames, Surrey KT1 2EE.