DATA PROTECTION PROCEDURE

Related College Policies:	**Data Protection Policy** https://www.kcl.ac.uk/governancezone/GovernanceLegal/Data-Protection-Policy.aspx **Records Management Policy** https://www.kcl.ac.uk/governancezone/InformationPolicies/Records-and-Information-Management-Policy.aspx **IT Acceptable Use Policy** https://www.kcl.ac.uk/governancezone/informationpolicies/it-acceptable-use-policy **Research Data Management Policy** https://www.kcl.ac.uk/governancezone/Research/Research-Data-Management-Policy.aspx
Related Procedures:	**Data Breach Management Procedure** https://www.kcl.ac.uk/governancezone/governancelegal/data-breach-procedure **Requests for Personal Information Procedure** https://www.kcl.ac.uk/aboutkings/orgstructure/ps/audit/compliance/data-protection/Requests-for-Personal-Information.aspx

---

SECTION 1: Implementing the Data Protection Policy

1. The university will only use personal data where strictly necessary, and will rely on an appropriate lawful basis for processing personal data

1.1 As an academic institution, employer and service provider, the university collects personal data when registering students, employing staff and providing services to customers. The university will only collect and use personal data where strictly necessary.

1.2 The university must have a valid lawful basis to process personal data. The university will satisfy at least one of the six available lawful bases (See Section 2), contained in data protection legislation, before processing any personal data.

1.3 Consent to process data will only be relied upon as the lawful basis when individuals have a real choice and control over the processing. Requests for consent will be prominent and separate from other terms and conditions. Consent will be based on a positive opt-in; pre-ticked boxes and other opt-out methods of consent will not be used. Explicit consent (one of the conditions available for processing special category personal data) will be based on a clear and specific statement of consent. Individuals will be given the ability to withdraw their consent at any time.

1.4 If the university offers online services directly to children, it will only seek consent if it has age-verification measures (and parental-consent measures for children under-13) in place.

1.5 The university will keep a record of when and how it obtained consent from individuals, and what they were told at the time.

1.6 When the university processes special category personal data, it will also identify a condition contained in data protection legislation for processing such data (see Section 2).

2. The university will inform people of the lawful basis and explain the purpose and manner of the processing in the form of privacy notices and other similar methods

2.1 The university will, at the time the data is obtained, provide information to individuals about why their personal data is needed, the lawful basis for the processing and how it will be used, typically through a privacy notice.

2.2 Privacy notices will be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

2.3 Individuals will be informed at the point of collection when there is an intention to use their personal data for marketing or other additional purposes and will be asked to provide their consent by actively opting in.

2.4 The university will not carry out automated decision-making or automated processing (including profiling) when a decision has a legal or similar significant effect on an individual unless:

- a data subject has explicitly consented;
- the processing is authorised by law (this ground cannot be used for special category personal data); or
- the processing is necessary for the performance of, or entering into, a contract (this ground cannot be used for special category personal data).

2.5 If a decision is to be based solely on automated processing (including profiling), then data subjects must be informed when the university first communicates with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

2.6 We must also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision. In accordance with paragraphs 8.6 and 8.7, a data protection impact assessment must be carried out before any automated processing (including profiling) or automated decision-making activities are undertaken.

3. The university will keep personal data secure and manage incidents effectively when things go wrong

3.1 The university will process personal data in a manner that ensures its security. Appropriate technical (e.g. encryption, access control) or organisational (e.g. policies and procedures, training) measures will be used to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.2 The university will maintain an Information Security Policy and an associated framework of technical support and guidance. Physical and technical security breaches, including data breaches, will be monitored and subject to routine reports and action by the Security Review Group.

3.3 Where it is lawful to do so, the university may access user accounts and intercept communications on its systems for legitimate purposes (e.g. to investigate suspected misuse), under the terms specified in the university's IT policies.

3.4 The university will follow a data breach management procedure for addressing data breaches. All suspected and actual data breaches will be reported to info-compliance@kcl.ac.uk as soon as possible.

3.5 The university will, where feasible, notify the Information Commissioner of a data breach within 72 hours of becoming aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of any individuals. It will also notify affected individuals about a breach without undue delay when it is likely to result in a high risk to their rights and freedoms. The risk level of a breach will be determined using the severity assessment tool in the breach management procedure.

3.6 A termly report of any serious data breaches will be made to the Security Review Group and the Audit, Risk and Compliance Committee.

4. The university will observe the rights of individuals

4.1 The rights of data subjects under data protection legislation will be respected and supported. Individuals have several rights under data protection legislation, including the right to have their personal data rectified, erased and restricted; the right to move, copy or transfer their personal data in electronic form; the right to object to processing; and rights relating to automated decision-making and profiling.

4.2 The right of access to personal data gives individuals the right to access their personal data and supplementary information and to be made aware of, and verify, the lawfulness of the processing. The university will respond without delay and no later than one month after receipt of the request, subject to ID verification and any applicable exemptions. All access requests will be dealt with in accordance with the university's published procedure.

5. The university will ensure staff are trained appropriately and advised on managing personal data

5.1 The Data Protection Officer is responsible for ensuring compliance with data protection legislation by providing advice, guidance and training to the university.

5.2 All staff must complete the university's mandatory online data protection training course within one month from the date of commencing employment and thereafter every two years.

5.3 Completion rates will be monitored by the Data Protection Officer and reported to senior managers at regular intervals. Failure to complete the mandatory training, in accordance with paragraph 5.2, will constitute a breach of this procedure and the Data Protection Policy and may result in disciplinary action.

5.4 The data protection pages of the staff intranet will feature guidance and practical information for staff around data protection.

5.5 The data protection pages of the university's website will feature the Data Protection Policy and procedures relating to implementation of the policy.

5.6 Staff and data subjects can contact the Data Protection Officer and the Information Compliance team by phone (020 7848 7816) or email (info-compliance@kcl.ac.uk) with any data protection queries.

5.7 Face-to-face, tailored training sessions are available from the Data Protection Officer and the Information Compliance team, on request and subject to availability.

6. The university will ensure that records containing personal data are managed effectively

6.1 The university will seek to maintain standards of data quality and avoid duplication, inaccuracies and inconsistencies across personal data sets by utilising master data management principles wherever possible. Master data management is the practice of defining and maintaining consistent definitions of widely used business critical data (or master data sets), then making these definitions available to be used in multiple IT systems across an organisation. Master data is likely to come from the central student, HR and finance systems. For example, student addresses and qualifications.

6.2 The university will implement a data steward and data custodian framework to enable clear lines of data ownership and accountability.

6.3 The university's records management policy and records retention schedule will be followed to help avoid excessive retention or premature destruction of personal data.

7. The university will only share personal data with third parties where adequate standards of data protection can be guaranteed and, where necessary, contractual arrangements are put in place

7.1 Whenever the university uses a data processor, it must have a written contract in place so that both parties understand their responsibilities and liabilities.

7.2 The university will use its own data protection legislation-compliant standard contract clauses whenever possible to ensure its contracts are consistent and compliant. Any substantial deviation from these clauses must first be checked with the Data Protection Officer.

7.3 The university is liable for its compliance with data protection legislation and will only appoint data processors who can provide sufficient guarantees that the requirements of data protection legislation will be met, and the rights of data subjects protected.

7.4 The university will not transfer personal data to countries outside the European Economic Area unless:

- the European Commission has issued a decision confirming that the country ensures an adequate level of protection for the data subjects' rights and freedoms;
- appropriate safeguards are in place, such as standard contractual clauses approved by the European Commission or an approved certification mechanism (e.g. the EU-US Privacy Shield Framework);
- the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between the university and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for the university's legitimate interests. For further guidance, see the GDPR guidance page.

7.5 Third parties (such as law enforcement bodies) may ask the university to disclose information relating to an individual for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Such requests should be made formally in writing (law enforcement bodies should submit their 'data protection request' form). The request should then be considered against the university's obligations under the data protection legislation, using a data protection impact assessment where appropriate (see paragraphs 8.6 and 8.7).

7.6 In urgent and emergency situations, the steps in paragraph 7.5 may be bypassed if it is deemed necessary and proportionate to do so. This judgement should be based on the risks of not sharing the data; keeping in mind data protection legislation does not prevent the sharing of data in situations where there is a danger to the health of a person.

8. The university will implement comprehensive but proportionate governance measures to demonstrate compliance with data protection legislation principles

8.1 A termly report on data protection compliance will be made to the university's Audit, Risk and Compliance Committee of the Council.

8.2 The university has appointed a Data Protection Officer to inform and advise the university about its obligations to comply with data protection legislation, to monitor compliance, and

to be the first point of contact for the Information Commissioner and for individuals whose data is processed.

8.3 The Data Protection Officer (the Assistant Director of Business Assurance (Information Compliance)) will operate independently and report to the highest management level of the university.

8.4 The university will maintain a written record of its processing activities, which will be made available to the Information Commissioner on request. Records will be updated annually to reflect the university's current processing activities.

8.5 The university will implement measures that meet the principles of data protection by design (designing projects, processes, products or systems with privacy in mind at the outset) and data protection by default. Measures could include:

- Data minimisation
- Pseudonymisation
- Transparency
- Allowing individuals to monitor processing
- Creating and improving security features on an ongoing basis

8.6 The university will use data protection impact assessments to help identify and reduce the data protection risks of its projects and meet individuals' expectations of privacy.

8.7 The university will carry out data protection impact assessments when using new technologies and/or the processing is likely to result in a high risk to the rights and freedoms of individuals. This may include (but is not limited to) systematic and extensive processing activities, large scale processing of special category personal data, and the use of CCTV.

8.8 The management of personal data in research studies will be subject to review by the university's Research Ethics Committee and to approval by external regulators, as required. All research studies that include the processing of participant personal data must register on the university's research data protection portal KDPR.

SECTION 2: Lawful bases for processing personal data and conditions for processing special category personal data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever the university processes personal data:

(a) **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the university is processing data that falls under (e))

For guidance on each lawful basis, see the GDPR guidance page.

In order to lawfully process **special category personal data**, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9:

- The data subject has given explicit consent to the processing.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest.

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical.

- Note this is an edited list of Article 9 conditions and further conditions and required safeguards will be contained in the final provisions of data protection legislation.

For guidance on processing special category personal data, see the GDPR guidance page.

SECTION 3 – Data protection legislation principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

> "a) processed lawfully, fairly and in a transparent manner in relation to individuals;
>
> b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
>
> c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
>
> d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
>
> f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

For guidance on each principle, see the GDPR guidance page.