IC001: DATA PROTECTION POLICY

Policy Category:	Governance
Subject:	Compliance with data protection legislation
Approving Authority:	Senior Management Team
Responsible Officer:	President & Principal/designate
Responsible Office:	Office of the Chairman and College Secretariat
Related Procedures:	Data Protection Procedure https://www.kcl.ac.uk/governancezone/assets/governancelegal/data-protection-procedure.pdf 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
Related College Policies:	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
Effective Date:	5 December 2019
Supersedes:	7 October 2015
Last Review:	3 December 2020
Next Review:	25 May 2021

---

1. Purpose & Scope

1.1 This policy covers all university activities and processes in which personal data is used, whether in electronic or hard copy form.

1.2 This policy applies to all members of the university including staff, students and others acting for, or on behalf of, the university or who are otherwise given access to the university's information infrastructure.

1.3 This policy takes precedence over any other university policy on matters relating to data protection.

2. Definitions

2.1 The following terms are defined in data protection legislation:

- Personal data – any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier (e.g. name, identification number, location data or online identifier).

- Special category personal data – the following types of personal data (specified in data protection legislation) which are particularly sensitive and private in nature, and therefore more likely to cause distress and damage if compromised:
    - Racial or ethnic origin
    - Political opinions
    - Religious or philosophical beliefs
    - Trade union membership
    - Health related conditions (physical or mental health)
    - Sex life and sexual orientation
    - Commission or alleged commission of any criminal offence
    - Genetic data
    - Biometric data, where processed to uniquely identify an individual
- Data subject – the individual to whom the personal data relates
- Data controller – determines the purposes and means of processing personal data
- Data processor – responsible for processing personal data on behalf of a controller
- Data breach – a security incident that affects the confidentiality, integrity or availability of personal data. A data breach occurs whenever any personal data is:
    - lost;
    - corrupted;
    - unintentionally destroyed or disclosed;
    - accessed or passed on without proper authorisation; or made unavailable and this unavailability has a significant negative effect on the data subjects

3. Policy

3.1 King's College London ("the university") is committed to complying with the General Data Protection Regulation (GDPR) and any legislation enacted in the UK in respect of the protection of personal data (together "data protection legislation").

3.2 To do this, the university will:

a) Only use personal data where strictly necessary, and will rely on an appropriate lawful basis for processing personal data
b) Inform data subjects of the lawful basis and explain the purpose and manner of the processing in the form of privacy notices and other similar methods
c) Keep personal data secure and manage incidents effectively when things go wrong
d) Observe the rights of individuals under data protection legislation
e) Ensure staff are trained appropriately in managing personal data
f) Ensure that records containing personal data are managed effectively
g) 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
h) Implement comprehensive and proportionate governance measures to demonstrate compliance with data protection legislation principles

3.3 Further details on the meaning and the steps the university must take to comply with these points is contained in the Data Protection Procedure.

4. Roles and responsibilities

4.1 Every individual who works for, or on behalf of, the university must ensure that they have completed the university's mandatory online GDPR training course within the last two years. Individuals must also ensure any personal data they handle is processed in accordance with this policy and the data protection legislation principles (see Data Protection Procedure).

4.2 The Senior Management Team is responsible for approving this policy and assuring Council that the university meets its data protection legislation obligations.

4.3 The Data Protection Officer (the Assistant Director of Business Assurance (Information Compliance)) is responsible for:

- Informing and advising the university of its data protection obligations
- Monitoring compliance
- Awareness-raising and training of staff involved with processing operations
- Undertaking internal audits of data protection
- Providing advice on data protection impact assessments
- Cooperating with the Information Commissioner and acting as the contact point for any issues relating to processing

4.4 Heads of Services and Executive Deans are responsible for ensuring awareness of, and compliance with, this policy in their respective areas. In particular, they are responsible for ensuring their staff members have completed the university's mandatory online GDPR training within the last two years.

4.5 The Information Compliance team is responsible for:

- Maintaining this policy
- Providing guidance, support, training and advice on data protection compliance
- Processing all subject access requests for the university
- Supporting the responsibilities of the Data Protection Officer

4.6 The Information Security Steering Board is responsible for managing information security across the university. It does this with the support of its sub-group, the Information Security Review Group. The purpose of these groups is to review the information security landscape (both digital and physical), assess the university's performance and readiness, and ensure risk reduction, remediation and response.