# Overseas Registration Exam (ORE) Part 1
# Policy and Procedures

# Data Security Policy

## 1. INTRODUCTION

1.1. Personal information is information which relates to a living individual and from which they can be identified, either directly or indirectly.

1.2. Personal information at King's College London is held in or forms part of many records including candidate records, staff files and identifiable research data. Personal information is varied, diverse and often vitally important to the business and research interests of the university.

1.3. Personal information must be handled with care and in compliance with the Data Protection Act 1998 (DPA).

1.4. Funding bodies, ethics committees and legislation such as the Human Tissue Act 2004 may impose additional requirements on the handling of personal data.

## 2. SCOPE

2.1. This policy establishes the university's commitment to adhering to the Data Protection Act 1998. The university has procedures that aim to ensure that all staff, candidates and agents of the university who have access to any personal data held by or on behalf of King's College London are fully aware of and abide by their duties and responsibilities under the DPA.

2.2. This policy covers all university activities and processes in which personal information is used whether it is in digital, analogue or paper form.

2.3. This policy applies to all members of the university including staff, candidates and other acting for or on behalf of King's College London or who are otherwise given access to the university's information infrastructure

2.4. This policy should be read and interpreted in conjunction with other related university policies and published guidance.

## 3. NOTIFICATION

3.1. In compliance with the DPA the university will notify the Information Commissioner (statutory regulator for the Act) of the reasons why personal information is held and used. The university's

notification is broadly expressed and covers normal uses of data in connection with university activities.

## 4. PRINCIPLES

4.1. Management of personal information at the university will comply with the eight data protection principles set out in the DPA. These are as follows:

a) Personal information will be processed fairly and lawfully

> *Processing* means any form of use of personal data, including (but not limited to) collecting, storing, managing, destroying, analysing or publishing personal information. *Fairly* means with the consent of the information subject, or otherwise in accordance with conditions defined under the Data Protection Act 1998; and ensuring as far as possible that individuals are aware of how their information will be used. *Lawfully* means in compliance with the Data Protection Act 1998 and any other mandatory requirements.

b) Personal information will be collected for clear and specific purposes and will not be reused in incompatible ways

c) The collection and use of personal information will be limited to the minimum amount required. Information will be relevant and not excessive

d) Where personal information is in ongoing use it will be kept accurate and up to date, as far as reasonably possible

e) Personal information will be retained only for as long as it is needed and then confidentially destroyed. If information is kept for a long time or is archived permanently this will be for a valid reason

f) Personal information will be used in accordance with the rights of information subjects. Their right of access to their own information and their legitimate expectations of privacy will be respected

g) Personal information will be kept securely. It will be protected against unauthorised access and against accidental loss, damage and destruction

h) Personal information will only be transferred outside the UK with proper protection for the rights of information subjects or with their full consent, or as otherwise provided by the Data Protection Act 1998.

## 5. ACTIONS AND ACTIVITIES

In compliance with the data protection principles the university will undertake the following actions and activities.

5.1. Personal information collection and use

a) When personal information is collected, individuals will be told clearly who will have access to it, who will use it and how it will be used

b) The university will only use personal information where strictly necessary. In research studies for instance, anonymised data would be preferred

c) Individuals will be informed at the point of collection when there is intention to use their personal information for marketing and given the opportunity to refuse consent to direct marketing

5.2. Quality and retention

a) The university will seek to maintain standards of information quality and avoid duplication inaccuracy and inconsistences across personal information sets

b) The university will maintain a comprehensive corporate Records and Data Retention Schedule in order to help avoid excessive retention or premature destruction of personal information

c) The university will provide guidance and training to support the effective classification, organisation and management of records containing personal data

5.3. Access

The rights of information subjects will be respected and supported, in particular the right of subject access (which is the right of every individual to access the information that the university holds about them) will be facilitated in line with the published subject access requests procedure. This right is qualified by exemptions specified in the Data Protection Act 1998.

5.4. IT development projects

The university will routinely assess the data protection risks associated with all development work on the systems that process personal information to ensure that any new initiatives (such as a change to the HR records system, for instance) will not have a disproportionate impact on the privacy of identifiable individuals. Risk assessments and procedures form part of the Information Technology project management framework.

5.5. Security

The university will maintain an Information Security Policy and an associated framework of technical support and guidance and documentation. Security breaches are monitored and subject to routine reports and action.

The university may access user accounts and intercept communications on its systems for legitimate purposes (for example, to counter abuse) under the terms specified in the university Regulations.

5.6. Personal information transfers

Personal information will only be transferred to territories outside the European Economic Area where adequate standards of privacy protection can be guaranteed, either by national laws or via contractual arrangements, and in other circumstances where transfers are permitted by the Data Protection Act 1998.

5.7. User Support

The university will provide freely accessible guidance, support and training on personal information management to all members of the university including staff, candidates and others acting for or on behalf of King's College London.

## 6. MAINTENANCE AND REPORTING

6.1. Methods of managing personal information (including in enterprise applications such as the candidate records database) are periodically reviewed.

6.2. The management of personal information in research studies is subject to review by an appropriate ethics committee and to approval by external regulators as required.

6.3. The number of subject access requests received by the university is reported monthly and compliance is monitored

6.4. A termly report on personal information management throughout the university is made by the Director of Governance and Legal Services to the Audit and Compliance Committee of the university Council.

6.5. A termly report of any personal data security breaches and on staff compliance with mandatory data protection training is made by the Head of Information Management and Compliance to the university's data Governance and Strategy Group.

## 7. ROLES AND RESPONSIBILITIES

7.1. The Data Governance and Strategy Group is responsible for approving this policy, and for monitoring its implementation to ensure continual improvement

7.2. Heads of Service and Executive Deans are responsible for ensuring awareness of and compliance with this policy in their areas

7.3. The IT Directorate's Network Security Team is responsible for maintaining the university's Information Security Policy in liaison with the Information Management and Compliance Team and specifically for the IT Security Framework and associated technologies and standards.

7.4. The IT Directorate and Library Services and responsible for the regular updating of the Library Services and Information Technology Services Regulations which form part of the university's Regulations and set out behaviours which are regarded as appropriate or breaches of discipline.

7.5. Personal responsibilities

a) Principle investigators are responsible for personal information management in their own research studies and for ensuring that secure information systems and operating procedures are in place with regards to data handling. Where personal data is processed, research staff and candidates must adhere to the personal data processing requirements set out in this policy as well as the University's Research Data Management Policy.

7.6.

a) Everyone who handles personal information for or on behalf of the university including staff, candidates, contractors and agents, is responsible for its safety and security and for personal compliance with the DPA. This includes personal responsibility for notifying the Information Management and Compliance Team promptly about any security breach of data loss affecting personal information whether generated within the university or in a related organisation such as NHS trust.

b) Failure to respond appropriately to a subject access request is a breach of the law. In particular, it should be noted that it is an offence to conceal, destroy or alter information to prevent it from being released, where the information is subject to a request.

c) Mishandling of personal information in any capacity is a breach of this policy and the university's Regulations and may additionally be a breach of the law.

d) Serious breaches of this policy (or repeated minor breaches) will be dealt with under the university's disciplinary procedures.