IT Acceptable Use Policy
Information Security Procedures

Effective Date:	May 2019
Supersedes:	November 2015
Last Review:	January 2023
Next Review:	January 2024

1. Purpose & Scope

1.1 This procedure underpins the IT Acceptable Use Policy in relation to Information Security. It sets out how King's College London will meet its obligations to preserve the confidentiality, integrity and availability of information used across the university.

1.2 The purpose of this procedure is to maintain a secure environment to create, use and store information. It also intended to support the university in maintaining compliance with all relevant legal and regulatory obligations.

1.3 This procedure applies to all staff, faculties and departments of the university, students and third parties.

1.4 The procedure applies to information held by the university regardless of the format in which it is held.

2. Procedure

2.1 User Responsibilities and Training

2.1.1 Anyone who handles personal data must do so in accordance with data protection legislation and the university's data protection policy together with all associated policies, procedures, standards and guidance.

2.1.2 All users must have completed any mandatory data protection training required of them. Online data protection training is provided by the university and is accessed through the Data Protection intranet site.

2.1.3 All users must adhere to the IT Acceptable Use Policy to ensure their actions are lawful, reasonable and raise no unnecessary risks or security threats for the university. This includes:

- Keeping credentials secure
- Use of email
- Use of encryption
- Using mobile devices
- Remote access
- Maintaining confidentiality of data
- Compliance with Payment Card Industry Data Security Standard

2.2 Risk Assessment

2.2.1 All areas of the university are required to perform a risk assessment as part of the annual business planning round. This must include risks relating to the vulnerability of information content and systems, as well as current threats.

2.3 Data Classification

2.3.1 Data must be classified appropriately to enhance information security and to aid understanding of the level of sensitivity accruing to a particular data set. This in turn will establish who should access it and what protections are needed to prevent that data being disclosed, altered or destroyed without authorisation.

2.3.2 Detailed guidance on the classification of data is available in the Data Governance Policy and the Information Classification Guide.

2.4 Retention and Disposal of Information

2.4.1 Retention and disposal of university information is addressed in the university Records Management Policy and related documents including the university's Records and Data Retention Schedule.

2.4.2 Appropriate procedures for information disposal must be made at a departmental level with support and guidance from King's Archives and Corporate Records Management team as required.

2.5 Reporting Security Incidents

2.5.1 Any suspicious IT related events or suspected cyber-attacks, or suspected security incidents which may involve loss or compromise of information must be immediately reported to IT via the service desk (8888@kcl.ac.uk or 0207 848 8888).

2.5.2 Any user who identifies a breach or a potential breach which may compromise personal data, must also notify the Information Compliance team immediately. The form for reporting a breach can be found on the intranet.

2.6 System Security

2.6.1 Systems and services should be configured with a minimum baseline in accordance with the Code of Connection Procedure.

2.6.2 Group shared or generic accounts, passwords or other authentication methods are prohibited for use of Highly Restricted Information (as defined in the Information Classification Procedure).

2.7 Business Continuity

2.7.1 Information security forms part of wider business continuity planning within the university. Data owners must:

- Regularly review and assess information security requirements.

- Ensure that information is properly backed up and can be restored in the event of an emergency. (See Business Continuity and Emergency Management policy).

2.8 Disposal of Equipment

2.8.1 Waste electrical and electronic equipment belonging to the university must be disposed of in a secure and sustainable manner. A contract with a third-party disposal specialist is in place to support this requirement. Detailed information about equipment disposal can be found at Electronic & Electronic Equipment Waste Recycling.

2.8.2 In accordance with the contractual obligations imposed by IT equipment vendors, the university will not allow staff members to take personal ownership of computer equipment which is no longer required.

2.8.3 Computer equipment must not be donated to third-party organisations, including charities, without the recorded permission of the relevant owner as identified in the asset register. If permission is granted, all data belonging to the university must be removed from the equipment in accordance with the UK Data Protection Act 2018 and the business requirements of commercial confidentiality.

3. Information Security Roles and Responsibilities

3.1 The **Senior Vice-President (Operations)** has ultimate responsibility for information security policies and guidance.

3.2 The **Data Protection Officer** helps the university to monitor internal compliance, inform and advise on its data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority.

3.3 **Data Stewards** are appointed to oversee discrete sets of data owned by the university. These data sets will broadly relate to the work of business units within the university, such as “people data”, “student data” or “financial data”. They may appoint Data Custodians as required to assist in the execution of the data strategy, policy and procedures for their area of stewardship.

3.4 The **Head of Cyber Security** will establish and maintain a security strategy for the university’s IT service and provide professional guidance to executive leadership. This will include recommending security solutions which mitigate risks, strengthen defences, and reduce vulnerabilities.

3.5 The **Information Compliance team** are responsible for the university’s compliance with data protection and access to information legislation and provide advice and guidance to the university on legislative and regulatory requirements relating to data protection.

3.6 The **IT Assurance team** assess information and security risks and identify and implement controls to risks and provide input into new or changes to existing policies and procedures. Where necessary, this team contributes to investigations relating to security incidents and recommends remedial actions.

3.7 The **Estates & Facilities Directorate** will have responsibility for collaborating with IT to provide a secure environment in which information can be protected and safeguarded.