# IT Acceptable Use Policy

| | |
|---|---|
| **Policy Category:** | General |
| **Subject:** | Use of university IT equipment, systems, and resources |
| **Approving Authority:** | SMT |
| **Responsible Officer:** | Senior Vice-President (Operations) |
| **Responsible Office:** | IT |
| **Related Procedures:** | Password Procedure<br>Email and Collaboration Tools Procedures<br>Mobile Device Procedure<br>Information Security Procedures<br>Data Protection Procedure<br>Code of Connection Procedure |
| **Related College Policies:** | Identity Management Policy<br>Records Management Policy<br>Data Protection Policy<br>Mobile Device Policy<br>Records Retention Schedule |
| **Effective Date:** | 22/09/2022 |
| **Supersedes:** | April 2022 |
| **Last Review:** | 20/12/2023 |
| **Next Review:** | 20/12/2024 |

---

**I. Purpose & Scope**

1.1 King's College London (the university) provides IT services primarily for academic and operational purposes to support learning, teaching, and research. IT services must be used responsibly, in accordance with the law and university policies in ways that do not raise unnecessary risks or security threats or bring the university into disrepute. This policy stipulates the practices and constraints that apply when accessing and using the university's IT services.

1.2 This policy applies to:

- students, researchers, academics, affiliates, staff, or partners who access the university's IT services on university owned and personally owned devices.
- all forms of IT services administered or supported by the university, including IT services provided under contract.
- the use of the university's hardware, software, network storage, data, and resources.
- all information held by the university regardless of the format in which it is held

1.3 This policy complies with the JANET Acceptable Use policy.

1.4 King's has a statutory duty, under the Counter Terrorism and Security Act 2015, termed 'PREVENT'. The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

**II. Definitions**

**1. Definitions of Unacceptable Use**

This list comprises of examples and is not meant to represent a comprehensive totality

- Creation, transmission and/or storage of any illegal, obscene, or indecent data in any format unless specifically in relation to academic projects, approved by the relevant department and having gone through scrutiny.
- Accessing, using or creating material intended to aid an illegal activity
- Any action that will bring the University, or its good name, into disrepute
- Deliberate unauthorised access to a third parties' account
- Downloading and/or distributing copyright protected or sensitive material
- Actions that deliberately waste IT time and effort and/or effects the security, integrity or performance of the KCL network.
- Connecting unauthorised hardware to the KCL network that may compromise the security and integrity of said network
- Circumventing, or attempting to circumvent, the KCL security systems
- Wantonly misuse, damage or sell/gift IT Assets

**2. Definitions of terms used within this policy**

| | |
|---|---|
| IT Service | An IT service is one based on the use of information technology and supports the institution's academic and business processes. At King's, IT service is made up of a combination of people, processes and technology. IT services provided under contract are defined as services provided by a third-party organisation outside of the university. Examples of IT services are officially sanctioned university IT products , telephony services and help desk functions. |
| University system | any university system or application which supports the university's academic and business processes, e.g. SITS, finance system, HR system, KEATS. |
| 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. |

| | |
|---|---|
| Auto-forwarding/ Redirecting email | this is the capability of automatically forwarding incoming email messages from one user account to another user account. |
| Remote Working | working from a remote location by electronically linking to the university systems. |
| Local jurisdictional law | The system of rules which the country you are working in recognises as regulating the actions of its members and which it may enforce by the imposition of penalties. |
| Virtual Desktops | Preconfigured images of operating systems and applications in which the desktop environment is separated from the physical device used to access it. Users can access their virtual desktops remotely over a network. |
| Mobile Device | A portable computing device (e.g. smart phone, tablet, laptop, portable storage device). |
| Information security | Refers to the procedures, processes and guidance which are designed and implemented to protect university information from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption. |
| Physical and environmental security | The protection of personnel, premises, facilities, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to the university. For example, this includes protection from (but not exclusively) fire, flood, natural disasters, burglary, theft, vandalism and terrorism. |
| Encryption | Used to protect individual documents, folders or even entire hard disk drives on mobile devices. |
| JANET | The name given to the electronic communications network and associated electronic communications networking services and facilities that support the requirements of the UK education and research communities. Organisations in the UK education and research communities use JANET to fulfil, and to undertake activities supporting, their missions of providing education, research, and business and community engagement. |
| SOE | Standard Operating Environment – devices owned by the university, procured, distributed and managed by King's IT |

## III. Policy

### 1. King's Credentials: Username, Password and Authentication Measures

1.1 Users must take all precautions to safeguard their usernames, passwords and any other IT credentials issued to them. They must not allow anyone else to use their IT credentials. Users will be held responsible for all activities undertaken using their credentials.

1.2 Users must not attempt to obtain, use, or disclose anyone else's credentials. Users must not impersonate someone else or otherwise disguise their identity when using the IT facilities.

1.3 Passwords must be unique to the system being used and conform to guidance regarding length and complexity established by the IT department (see Password Procedures), where single sign on isn't applicable.

1.4 Where applicable to the system, the university requires users to authenticate their identity through Multi-Factor Authentication (MFA) technology, this should be set up within the university recommended timeframes. To access those systems where MFA technology has been enabled, users will be required to provide unique information sent to them via an independent method such as an authenticator application, SMS message to a pre-registered mobile device or a similar alternative method supported by the university, in addition to their username and password.

## 2. Accessing and Using University Systems

2.1 Only users who have successfully completed the mandatory training programmes including data protection and security training should access university systems and information. All users are required to complete the necessary training programmes on initiation and again every 12 months thereafter.

2.2 Any access or attempt to access university systems and information for which permission has not been granted will be treated as a disciplinary offence.

2.3 Access to university systems and information must be under the following:

- **Through a managed, trusted SOE (standard operating environment) device** supplied by the university's IT Service wherever the option to use one exists.
- **Using Your Own Device,** providing it conforms to the standards as laid out in the Bring your own device (BYOD) procedure.
- **Compliant with the university's Code of Connection**, which is set out in the relevant procedure

2.4 Access to university systems and information should be via a trusted network. Public Wi-Fi (in hotels for example) should be avoided. If there is no other option but to use public WiFi, users should establish a VPN connection via a solution approved by the IT Cybersecurity team. Windows KCL SOE devices provide this requirement via Windows Remote Access VPN (WRA) and Forticlient VPN. Access to Forticlient can be arranged via the IT Service Desk. Non-SOE devices are not covered by WRA but users can request the addition of Forticlient VPN onto a personal device by contacting King's IT Service Desk.

2.5 Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The university reserves the right to block or monitor access to such material

2.6 Any member of staff working remotely is responsible for ensuring that they work securely and protect both university information and university-owned equipment from loss, damage or unauthorised access. Users must abide by local jurisdictional law when remotely accessing any KCL systems.

## 3. Information Security

3.1 All users of the systems must immediately report any suspected breaches, cyber-attacks, or security related issues via the IT Service Desk and, in the case of a breach that may compromise personal data, must also notify the Information Compliance team immediately. Please see the guidance for reporting a breach.

3.2 Individuals who handle personal, confidential, or sensitive information must take all reasonable steps to safeguard it and must be aware of and observe the requirements of the university's Data Protection Policy and its related procedures. Any breaches of confidence relating to confidential information held by the university may be treated as a disciplinary offence (under either staff or student disciplinary procedures) and may constitute an offence under data protection legislation or regulations.

3.3 University managed laptops (SOE devices) will be encrypted as standard. To guarantee the security of the device, encryption must always remain enabled.

3.4 Non-SOE and BYOD devices should be encrypted if used for accessing King's systems and data. For advice on encryption, please contact the IT Service Desk.

3.5 The university reserves the right to delete or remove user data from central IT Assets (such as old user profiles on an SOE laptop) after 1 year, as per the retention policy.

## 4. University Owned Computing Equipment

4.1 Users who are issued university owned equipment (including mobile devices) are responsible for that equipment. They must take all reasonable steps to protect and secure the equipment and any data stored on it as outlined in the Data Protection Policy, Data Breach Management Procedure, and Mobile Device Policy.

4.2 Users must manage the consumption of data on their university owned mobile devices to remain within the limits set and prevent additional costs being incurred.

4.3 Users are responsible for the return of all university owned equipment when leaving the university's employment, or on demand by the head of department, HR or university IT Services. Individuals who do not return equipment may be legally pursued by the University.

## 5. Personal Use

5.1 Whilst a reasonable level of personal use of IT devices and systems is permissible, users must not routinely use King's systems and devices for personal use. Personal use must not interfere with university business or the performance of university systems.

5.2 Users must ensure that their personal use of devices does not lead to consumption of data beyond set limits.

5.3 Users must ensure that their personal use does not lead to any information security risks, data loss or data breach.

## 6. Email and Instant Messaging

6.1 This policy covers the use of university email accounts assigned to individuals or groups, and instant messaging via university provided means. It also applies to other electronic software based collaborative tools that may be used by the University.

6.2 Users must follow the guidance regarding the use of emails as stated in the Email and Collaboration Tools Procedures

6.3 The use of email and instant messaging must in all ways meet the conditions of the university's policies concerning communications, dignity, equality, diversity, inclusion and respect.

6.4 Emails and messages sent using university provided means are owned by King's College London. They are searchable, auditable and usable in situations such as (but not limited to) legal proceedings, internal disciplinary proceedings, Freedom of Information (FOI) requests and Subject Access (SAR/DAR) Requests.

## 7. Monitoring and IT Access

7.1 The university monitors and records the use of its IT facilities for various purposes including:

- The effective and efficient planning and operation of IT facilities
- Detection and prevention of infringement of this policy, related procedures and relevant legislation
- Investigation of alleged misconduct
- Compliance with lawful requests for information from government and law enforcement agencies.

7.2 The CIO, on the recommendation of the Head of Department or Director of HR, may authorise access to a user's accounts for any of the reasons noted above or to permit ongoing university operations in the event of the death, incapacity, suspension, dismissal, departure or long-term absence of a user.

## 8. Enforcement

8.1 Following the requirements of this policy, other associated policies and procedures will ensure that users comply with the law. However, users should contact the IT Service Desk for advice about any concerns.

8.2 Non-compliance with this procedure or associated policies and procedures is an infringement of King's regulations and will be investigated in accordance with the appropriate university regulations.

8.3 The CIO or designate may remove or limit a user's access to the university's systems on a temporary basis when that is deemed necessary to protect the system or prevent reputational damage to the university or in the course of an investigation.

8.4 On the recommendation of the CIO or designate, further access limitations or permanent denial of access may be imposed by the Senior Vice-President (Operations) or designate.

## 9. Review

9.1 This policy shall be reviewed at least every three years.

**Appendix A – Change log**

| Version | Date | Name | Role | Changes made |
|---|---|---|---|---|
| 3.1 | 21/04/23 | Lauren Middlemist | IT Assurance Apprentice | Addition to IT Service definition - Examples of IT services are officially sanctioned university IT products, telephony services and help desk functions<br><br>Change log added as Appendix A |
| 3.2 | 20/12/23 | JEH | ITAO | Interim Review |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |