Code of Connection Procedure

Effective Date:	22/09/2022
Supersedes:	N/A
Last Review:	11/12/2024
Next Review:	11/12/2025

I. Purpose and Scope

1.1 The purpose of this document is to define the code of connection for every user who connects directly to King's College London university wired and wireless network. This Code of Connection supports the Information Security Policy and Data Protection Policy by establishing a minimum security baseline. This code defines the actions users must take whilst connecting to the university infrastructure via university owned devices to preserve the security and integrity of the data managed by the university, as well as connecting in a manner that does not extend any of the KCL networks, impact performance, resilience and availability of the infrastructure.

1.2 This document applies to any user who connects directly to the university infrastructure regardless of the status of the user or how the device is managed.

1.3 This document does not cover Bring Your Own Device (BYOD). See BYOD procedure

1.4 The university strongly suggests the use of SOE for end user devices and centrally managed solutions. Non-SOE devices should only be used where an SOE is not possible. Non-SOE devices broadly fall into three categories:

1. Computers (desktop/laptop/server) managed by local/departmental IT support group/person. The local/departmental IT support group/person are responsible for ensuring compliance.
2. Computers (desktop/laptop/server) managed by individual researcher. The individual researcher is responsible for ensuring compliance.
3. Computers (desktop/laptop/server) managed by 3rd party providers e.g., desktop computer integrated with scientific instrument. These devices should be identified to e-Research and King's IT who will support the owner to determine whether compliance is possible and if not implement mitigating security controls while keeping the system operational.

1.5 For advice and guidance on adhering to any sections of this procedure, please see our dedicated Sharepoint site .

1.6 Definitions of key terms used in this procedure can be found at the bottom of this document.

II. Related Policies and Procedures

- IT Acceptable Use Policy
- IT Acceptable Use Policy – Password Procedure
- IT Acceptable Use Policy - Bring Your Own Device (BYOD) Procedure
- Data Protection Policy
- Data Protection Procedure
- Data Governance Policy
- Data Governance Procedure
- Data Breach Management Procedure
- Records Management Policy
- Research Data Management Policy
- Patch Management Policy

III. Definitions

Applications	A computing program or piece of software designed to fulfil a particular purpose
BYOD	Bring your own device
Critical Systems	Systems which are essential to the services provided by and day to day running of the university
Device	A piece of portable electronic equipment that can connect to the internet, especially a smartphone or tablet computer.
Hardware Assets	Any tangible, physical company technology asset, including those currently in use, those in storage, and support equipment.
Incident	An unexpected event that disrupts business operational processes or reduces the quality of a service.
IT Equipment	Any information technology equipment, irrespective of owner
Inherent Vulnerability	Vulnerabilities that are present before any security procedures are implemented
Malware	A software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system
Multi-Factor Authentication (MFA)	A security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction. For example, logging into Microsoft Teams and having to input a code from the Microsoft Authenticator App/text message/phone call to prove your identity and gain access to the system.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions.
SOE	Standard Operating Environment – university owned and managed devices. For example: the laptops provided to staff by King's IT.

Software Assets	All Software, data rights, documentation and associated license, escrow, support and maintenance agreements provided by the university for work purposes
University System	Defined as any university system or application which supports the university's academic and business processes, e.g., SITS, finance system, HR system, KEATS
VLAN	Virtual local area network
Verified	Known, assessed, and approved by King's IT
Unverified	Unknown and unassessed by King's IT

2. Procedure

2.1 Inventory and Control of Hardware Assets

2.1.1 All computing equipment and systems must have a designated, current and contactable owner.

2.1.2 Inventory control of SOE devices is managed by King's IT. Non-SOE devices purchased by an individual department are the responsibility of that department and should be logged in a record such as that in Appendix 1 of this document, so that when requested, information can be supplied to King's IT for reasons such as (but not limited to):

- Legal procedures
- Internal disciplinary procedures
- Information security incidents

If you are unsure of who would be responsible for your inventory or would like an example template, please check our dedicated Sharepoint site.

2.2 Inventory and Control of Software and information Assets

2.2.1 Software installed via standard installation packages should be reportable to IT. Users should be able to provide details of their inventory upon request by IT.

2.3 Vulnerability (patch) Management

2.3.1 All IT equipment and systems must be patched in accordance with the IT Patch Management Policy.

2.3.2 Any exceptions must be requested & approved via e-Research and/or IT Assurance who will provide guidance.

2.4 Secure Configuration

2.4.1 All IT systems, software and services are configured to reduce the level of inherent vulnerability. We will have ensured that applications, services, processes and ports not required are disabled by default.

2.4.2 Default passwords and usernames must be changed immediately upon first configuration.

2.5 Malware protection, monitoring and intrusion detection

2.5.1 All staff have a duty to prevent the introduction of malware to the network to prevent harmful code from causing damage or accessing sensitive data.

2.5.2 Managed and regularly updated malware protection systems should be used where possible. IT services may deploy agents to help manage and evidence this. Please see our dedicated Sharepoint for guidance.

2.5.3 Users are expected to conduct reasonable due diligence when installing new software on non-centrally managed systems. For guidance please see our dedicated SharePoint page.

2.5.4 Users who identify potentially malicious software must contact the IT Service Desk immediately, taking care not to open, use or distribute the software before it has been properly assessed.

2.5.5 We must all restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data. Well managed and regularly updated malware protection systems should be used wherever appropriate.

2.5.6 For information on current Anti-Malware options available for you, please see here.

2.6 External exposure

2.6.1 External facing (i.e., being made available for inbound connections over the Internet) services, ports and interfaces will be limited to only those absolutely necessary to achieve the required purpose. Any users wishing to configure an externally facing service or system must obtain approval from IT Security, who will follow the standard governance processes, before any work is undertaken.

2.6.2 Any changes to an externally facing system or service that alter port configurations must obtain approval from IT Security before any change is made.

2.6.3 Wherever practical services will be hosted on centrally managed (i.e., IT or e-Research) platforms. In cases where this is not viable the security architecture of the application will need to be demonstrated to IT and/or e-Research prior to any firewall changes being made.

2.6.4 All devices must be placed behind KCL perimeter security protections and monitoring. Endpoint devices must not establish an external connection to facilitate a reverse inbound connection with the aim of exposing internal resources without explicit approval.

2.7 Authentication

2.7.1 Multi-factor authentication (MFA) must be used wherever it is available. See our dedicated Sharepoint for guidance on configuring MFA

2.7.2 All staff and students must adhere to the measures stated in the King's College London Acceptable Use Policy Password Procedure

2.8 Security Incident Reporting

2.8.1 Security related IT incidents or other suspicious activity must be reported immediately upon discovery via the IT service desk as per the Data Breach Management Procedure.

2.8.2 Where security incident response plans are used, plans need to have been tested and scrutinised to ensure timely action to contain any incidents, limit harm, ensure appropriate escalation. All response plans should be regularly reviewed to ensure that they improve over time. These plans will include named responsible owners and pre-defined processes to respond to common forms of attack.

2.8.3 Logs must be retained and appropriately secured for critical systems and data access to aid with incident investigations. Guidance on keeping logs and identifying critical systems can be found on our dedicated SharePoint page.

3. Governance and exceptions

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

3.2 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.

3.3 The university may remove or limit access to its systems on a temporary basis that is deemed necessary to protect the university infrastructure or to prevent reputational damage or in the course of an investigation.

3.4 The university reserves the right to investigate and interrogate any hardware, software or code which it deems to be connected to its network and systems. This includes all SOE and non-SOE devices.

3.5 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.

Appendix A – Change Log

Version	Date	Name	Role	Changes made
1.2	22/09/22	Kirsty Lynch	Senior IT Assurance Officer	Change Log added as Appendix A
1.3	20/12/23	Jim Hall	ITAO	Interim review