Identity Management Policy

Policy Category:	General
Subject:	Identity management for access to university systems
Approving Authority:	SMT
Responsible Officer:	Senior Vice-President (Operations)
Responsible Office:	IT Services
Related Procedures:	Identity Management Procedure
	Email and Collaboration Tools Procedure
Related College Policies:	IT Acceptable Use Policy
Effective Date:	May 2019
Supersedes:	July 2016
Last Review:	December 2024
Next Review:	December 2025

I. Purpose & Scope

1.1 The purpose of this policy is to ensure that accounts are held only by people who have an active association with the university and that users have access to their own personal data and to university systems required to undertake their studies, job or role at the university.

1.2 This policy applies to any individual who has access to the university's systems and services through an account in the university's Active Directory, or systems for IT services provided under contract, including:

- Students
- Researchers
- Members of staff with a contract of employment with the university and former members of staff with an ongoing association (emeritus or part time position) with the university
- Staff on temporary contracts, fixed term contracts or appointments approved by HR
- A recognised affiliate of the university – governor, volunteer, workforce member, visitor or supplier
- Staff in partner NHS trusts
- Staff in organisations who are provided with IT Services by the university (e.g. Institute of Hepatology, the Health Information Network, King's Maths Academy)
- Other individuals at the discretion of the university

II. Definitions

Identity is a means of identifying an individual through electronic means usually in the form of a unique username.

A **King's IT account** is an individual user account in the King's Active Directory.

A **King's username** is the log on name of the individual's Active Directory account. It is also known as the King's ID and informally as a "K number".

Active Directory is the 'directory service' portion of Windows operating system. Active Directory manages the identities and relationships of the distributed resources that make up a network environment. It stores information about network-based entities (e.g. applications, files, printers, people) and provides a consistent way to name, describe, locate, access, manage and secure information about these resources. It is the central authority that manages the identities and brokers the relationships between these distributed resources, enabling them to work together.

Access rights are defined as the ability to log in to a system or use a service (e.g. the wireless network), a privilege level within a system (e.g. read or read/write), or as access to elements of a system or service.

Authoritative system: This is the information storage system that is the principal data source for a given data element or piece of information. For Student IT accounts this is SITs. For workforce IT accounts this is the HR Management System.

MIM: Microsoft Identity Manager is a tool that allows organisations to manage users, access, policies and credentials.

Provisioning: The process for creating an IT account.

De-provisioning: The process for deactivating access from a system or service for an individual when they no longer qualify for access.

Types of accounts:

1. **Staff** for people employed by the university or any wholly owned subsidiary of King's College London
2. **Student** allocated to a person who is going to be, currently is or has been registered at the university to undertake a course of learning. This includes postdoctoral researchers.
3. **Affiliate** for people who work closely with but are not directly employed by the university.
4. **NHS Trust** account for NHS staff granted library access under the Library Services Agreement with the NHS Trusts.
5. **Guest** are created for temporary purposes such as conducting exams.

III. Policy

1. Risk

1.1 Compromised user credentials can often serve as an entry point into an organisation's network and its information assets. Identity management can be used to safeguard against the rising threats of ransomware, criminal hacking, phishing and other malware attacks.

2. Access Rights & Requirements

2.1 Individual users must agree to the university's IT Acceptable Use Policy before being assigned any identity with access rights to use university services and systems.

2.2 In addition, all staff must agree to the Data Protection Policy. For some business systems it may be appropriate for the user to agree an appropriate use declaration the first time they log on to the system.

2.3 A King's username is unique. Once assigned, IT will ensure it is never reassigned to identify another person.

2.4 Where an individual is a student and a member of staff, they will have separate accounts and usernames for each of the authoritative systems in which they appear.

2.5 All individuals will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.

2.6 For staff, access to systems must be available on day one. The only exceptions will be where additional training or approval is required.

2.7 For students, access rights will be governed by what type of course(s) a student is actively studying on. Where a student is studying on more than one course at the same time, the access rights applicable to all courses will be given.

2.8 Each combination of student status and course type will have a default set of access rights that have been agreed centrally.

3. Changes and Deprovisioning

3.1 Departments must ensure that IT are informed about any changes to an individual account holder's status and any required changes to or deprovisioning of individual accounts. Access for terminated staff or staff who have left the university should be immediately deactivated.

4. Source Systems and Data Quality

4.1 The Identity Management system is wholly reliant on the quality of data from its source systems and the timeliness of events within those systems to ensure that every user has the appropriate access rights at the correct time. It is the responsibility of the Data Steward of the source system to ensure that a high-degree of data quality is maintained and that the

system that holds that data is updated in a timely fashion. All data should be subject to data validation at the point of entry and periodic (at least annual) revalidation.

5. Enforcement

5.1 Within each function, an appointed Data Steward shall enforce this policy. Enforcement of departmental processes is the responsibility of the Head of Department.

6. Review

6.1 This policy will 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	Change control log added as Appendix A.
3.2	20/12/23	JEH	ITAO	Interim review
3.3	12/12/2024	Titus James	Collaboration & IDM Manager	Document review, no changes