ICT CoP 04: Account Security Management

Introduction

1.1 This Code of Practice defines the procedures and provides advice for managing and protecting passwords associated with all Information Systems at Imperial College London.

Selecting a strong password

2.1 Imperial enforces the following criteria in order for users to select a strong password, and therefore achieve effective password protection:

2.1.1 A password must be at least 12 characters in length.

2.1.2 A password must contain at least three of the following four elements:

- Numeric Characters (0 - 9)
- Uppercase Characters (A-Z)
- Lowercase Characters (a - z)
- Special Characters (?, !, @, #, %, etc.)

2.1.3 3 random words should be used to create your password.

1. A password must not contain any of the following:

- A name, of either a person or place that is easily associated with you.
- An easily guessable date, such as partner's birthday.
- Information related to you, such as your car number plate, NI number, CID number, etc.
- The same or close to your account username (including reversing or misspelling of the username)
- Any of the examples given on the ICT website, or this Code of Practice.

2.1.4 The new password cannot be the same as one of the last 24 passwords used.

2.1.5 If equipment/software is supplied with default credentials, then these should be changed prior to the deployment.

Protecting passwords

3.1 Users should choose a password that is memorable and avoid writing down passwords and under no circumstances leave a password in a place readily accessible to others.

3.2 Users should not disclose their password to others. ICT will never ask for a user's password. The only person who needs to know your password is you.

2. If you need to give another member of the university access to your mailbox then delegate access should be set up by contacting the ICT Service Desk.

3. Where shared mailboxes are in use, individuals should authenticate as themselves and use delegate access.

3.3 If a user becomes aware their password has been disclosed by accident or otherwise, they should change their password immediately and report it to ICT.

4. A user should take care that it is difficult for others to see their password being typed in. Care should be taken as to who is watching when the password is entered.

5. Users should not enter their passwords into a website, unless they are sure that it is a legitimate university system / website. The best method to ensure this is to access sites using your own bookmarks or typed-in URLs. Avoid using links especially from within emails claiming to be legitimate.

6. Default administrator passwords for all devices must be changed before any device is connected to the university network.

7. For shared accounts (e.g. system accounts), if any member of Imperial changes role or leaves the organisation, the password for the shared account should be immediately changed.

Multi-factor authentication (MFA)

4.1 MFA is used to enhance the security of all accounts requiring users to authenticate with something they know (username and password) and something they have (smartphone/hardware token);
4.1.1 ICT's recommended form of MFA is to use Passkeys via the Authenticator App.
4.1.2 ICT will provide hardware tokens where staff members do not want to use their personal phones for this purpose.

Changing passwords

5.1 Imperial users should change their passwords if they suspect that their credentials have been compromised and report it to ICT.
5.2 You can change your password by logging on to an Imperial computer and using the link on the following page: http://www.imperial.ac.uk/admin-services/ict/self-service/connect-communicate/user-accounts-passwords/change-reset-password/.
5.3 Recycling of old passwords is not allowed. This is a good practice you should also use for non-university systems.

5.4 Users with passwords not in compliance with this Code of Practice will be required to change their password immediately.

Passwords for non-university systems

6.1 You are advised to follow the best practices provided in this Code of Practice when choosing passwords for non-university systems.
6.2 You should not use your Imperial username and password for setting up accounts on websites or other Internet resources. It is also recommended that you do not use your Imperial email address for creating personal use.

Document Control

Document title:		ICT CoP 04: Account Security Management	
Version:	V6	**Date:**	September 2025
Initially approved by and date:		Provost Board / November 2016	
Version approved by and date:		Chief Information Security Officer / 04-09-2025	
Version effective from:		September 2025	
Originator:		Information and Communication Technologies	
Contact for queries:		Chief Information Security Officer	
Cross References:		Information Security Policy CoP 01 – Hardware and Software Asset management CoP 02 – Electronic Messaging CoP 03 – Inspection of Electronic Communications and Data CoP 05 – System Security CoP 06 – Conditions of Use of IT Resources	
Notes and latest changes:		January 2013 V1.0 - Approved April 2016 V1.1 - Fully revised version following findings report by Information Governance Audit in 2015 and Implementation of Microsoft Office 365 May 2016 V1.2 - Revised by IGSG and College Secretary July 2016 V1.3 - Reviewed by IGSG November 2016 V2.0 - Approved by Provost Board November 2017 V2.1 - Review by ICT IG Leads May 2018 V3.0 - Published version in light of GDPR implementation March 2019 V3.1 - Reviewed by ICT Governance and Security August 2020 V3.2 - Scope extended to cover account security January 2021 V4.0 - Published version linked to InfoSec Policy March 2022 V4.1 - MFA Added June 2022 V4.2 / V5.0 - The title of the code of practice changed from “password CoP” to “Account Security Management CoP”. - Removed password expiry requirement, increased password length to 12, recommended the use of 3 random words and to use delegate access to share inboxes, they should change their password if they suspect their password was compromised; not use their College password for personal accounts.	

	- V5.0 approved by IGSG February 2025 V6 - Updated to meet new brand standard - Removed all references to 'College'