Imperial College
London

Imperial College

Code of Practice 4: Passwords

Doc. Ref.	: Code of Practice 4: Passwords
Version	: 3.0
Status	: Approved
Date	: 01/05/2018
Approved by	: John Neilson, College Secretary
Review by	: 01/05/2019

1. 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.

2. SELECTING A STRONG PASSWORD

2.1 College 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 8 characters in length.

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

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

2.1.3 A password should not contain any of the following:

(I) A word, either from a dictionary (any language), slang or common acronym.
(II) A name, of either a person or place.
(III) An easily guessable date, such as partner's birthday.
(IV) Information related to you, such as your car number plate, NI number, CID number, etc.
(V) The same or close to your account username (including reversing or misspelling of the username)
(VI) 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 12 passwords used.

3. 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 the user.

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.

3.4 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.

3.5 Users should not enter their passwords into a website, unless they are sure that it is a legitimate college 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.

4. CHANGING PASSWORDS

4.1 College users are asked to change their passwords periodically. This is currently between 30 days and a year depending on roles and responsibilities of account holders.

4.2 You can change your password by logging on to a College 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/

4.3 Recycling of old passwords is not allowed. This is a good practice you could also use for non-College systems.

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

4.5 Users who are required to change their password will be contacted via email, telephone or in person by a member of ICT staff. Users should not reveal their passwords to anyone including ICT Staff.

5. PASSWORDS FOR NON-COLLEGE SYSTEMS

5.1 You are advised to follow the best practices provided in this Code of Practice when choosing passwords for non-College systems.

5.2 You should not use your College username and password for setting up accounts on websites or other Internet resources.

Version History

Version/Status	Release Date	Comments
1.0/Approved	January 2013	Approved
1.1/Draft	April 2016	Fully revised version following findings report by Information Governance Audit in 2015 and Implementation of Microsoft Office 365
1.2/Draft	May 2016	Revised as requested by ISSG. Reviewed by John Neilson, College Secretary and Mike Russell, CIO
1.3/In Review	July 2016	Reviewed by IGSG.
2.0/Approved	November 2016	Approved by the Provost Board
2.1/In Review	November 2017	Reviewed by Tim Rodgers, Okan Kibaroglu and Matthew Williams.
3.0/Approved	May 2018	Published version