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 12 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 3 random words should be used to create your password.

2.1.4 A password should not contain any of the following:

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

2.1.5 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.

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.

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

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

3.7 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.

4. MULTI-FACTOR AUTHENTICATION (MFA)

4.1 MFA will be used to enhance the security of accounts requiring users to authenticate with something they know (username and password) and something they have (smartphone/hardware token). ICT will provide hardware tokens where staff members do not want to use their personal phones for this purpose.

5. CHANGING PASSWORDS

5.1 College users should change their passwords if they suspect that their credentials have been compromised.

5.2 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/

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

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

6. PASSWORDS FOR NON-COLLEGE SYSTEMS

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

<table>
<thead>
<tr>
<th>Version/Status</th>
<th>Release Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0/Approved</td>
<td>January 2013</td>
<td>Approved</td>
</tr>
<tr>
<td>1.1/Draft</td>
<td>April 2016</td>
<td>Fully revised version following findings report by Information Governance Audit in 2015 and Implementation of Microsoft Office 365</td>
</tr>
<tr>
<td>1.2/Draft</td>
<td>May 2016</td>
<td>Revised as requested by ISSG. Reviewed by John Neilson, College Secretary and Mike Russell, CIO</td>
</tr>
<tr>
<td>1.3/In Review</td>
<td>July 2016</td>
<td>Reviewed by IGSG.</td>
</tr>
<tr>
<td>2.0/Approved</td>
<td>November 2016</td>
<td>Approved by the Provost Board</td>
</tr>
<tr>
<td>2.1/In Review</td>
<td>November 2017</td>
<td>Reviewed by Tim Rodgers, Okan Kibaroglu and Matthew Williams.</td>
</tr>
<tr>
<td>3.0/Approved</td>
<td>May 2018</td>
<td>Published version</td>
</tr>
<tr>
<td>3.1/In Review</td>
<td>March 2019</td>
<td>Reviewed by ICT Governance and Security</td>
</tr>
<tr>
<td>3.2/In Review</td>
<td>August 2020</td>
<td>Scope extended to cover account security in general</td>
</tr>
<tr>
<td>4.0/Approved</td>
<td>January 2021</td>
<td>Published linked to Info Sec policy v6.0</td>
</tr>
<tr>
<td>4.1/In Review</td>
<td>March 2022</td>
<td>Multi factor authentication added. &quot;Default password for devices must be changed&quot; added.</td>
</tr>
<tr>
<td>4.2/In Review</td>
<td>June 2022</td>
<td>The title of the code of practice changed from &quot;password CoP&quot; to &quot;Account Security Management CoP&quot;. 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.</td>
</tr>
<tr>
<td>5.0/Published</td>
<td>29 June 2022</td>
<td>Approved by the Information Governance Steering Group.</td>
</tr>
</tbody>
</table>