# Password Change Procedure - June 2018

| Document Control Information | |
|---|---|
| Reviewed by Senior Management Team: | FINAL |
| Date of Next Review: | June 2021 |
| Approved by: | SMT |

The persons/committee responsible for this document reserve the right to amend this document at any time should the need arise. All appropriate staff will be informed should this occur.

## BACKGROUND

Passwords are the easiest and most common way of verifying an identity to allow users access to the College network and its on-line resources. Passwords are also used to protect information from un-authorised access, change or deletion.

However College logins provide access to a number of important, and in some cases, confidential resources. Users logging into the college network have access to personal files in their home folder, access to shared files on the Z: drive, access to personal and shared e-mail and so on.

Users also have access to a growing number of on-line resources – student ILPs, student accounts password reset systems, OneDrive storage (again both personal and shared), wage slips, etc.

A strong password that is difficult for someone to guess or crack by brute force attack is therefore vital in order to safeguard the information that users have access to.

The information in this document – as well as the advice on creating secure passwords – is based on recommendations from the National Cyber Security Centre: Password Guidance: Simplifying Your Approach.

## THE COLLEGE PASSWORD PROCEDURE

a) Passwords must be at least 8 characters long.

a) They must include a mixture of characters containing at least one lower case letter, one upper case letter and one number.

b) You will be able to enter a maximum of 10 wrong passwords in a 5 minute period. After the 10th wrong password has been entered, the account will be automatically locked for 5 minutes, then immediately unlocked.

c) You will only be required to change your password if it is believed that the current password has been compromised, there are no regular forced password changes.

d) You will be prevented from using your last 5 passwords.

## HOW WILL THIS POLICY AFFECT ME?

There are three notable changes between the old and new polices:

1) The introduction of a lockout policy. This is to prevent the use of automated tools which can try huge numbers of password attempts in a very short period of time. If you do lock yourself out of your account your account will be activated after 5 minutes.
2) Regular, enforced, password changes are no longer required.
3) The length of the required password should now be 8 characters instead of 7.

NOTE: If you have your e-mail configured on a phone or tablet, again you will need to update the password on the email program for your device.

**If you fail to do this then the mail client will keep trying to access your account with the wrong password and therefore activate the lockout policy on your account!**

The same warning applies to phones or tablets connected to the College Wi-Fi – you will need to change the password on these devices to prevent them from locking your account by trying to use your old password to establish a connection.

## ADVICE ON CHOOSING SECURE PASSWORDS

The aim of this new policy is based on the idea of enabling users to create passwords which are easy to remember. However the **security** of this policy is based on the idea that users will also create passwords which are long enough to make them too long for password cracking software to be to do so in a short period of time.

With this in mind, here are some suggestions for creating long, but easy to remember, passwords:

- Use 4 random words - 1**HillBucketMonkeyOrange, MexicoFocusCoasterPencil2018, KeySandwich7Fork**

- Use a phrase - 1**IhateSoftBoiledEggs1, 1MondaysAreTheWorstDayOfTheWeek, 2times2isFour.**

- Use a line from a song, a poem, a proverb etc. – **H,D,D,T,M,R,U,T,C** (each letter, plus commas, from “Hickory, dickory, dock, the mouse ran up the clock).
  **C”H!”&lstDoW2018** (Cry “Havoc!” and let slip the dogs of war”)

- Use padding – take a “simple” word – Trampoline – and add some extra characters:
  before - **!”Trampoline**
  After – **Trampoline100()**

Remember, Remember, remember - The longer a password the better!

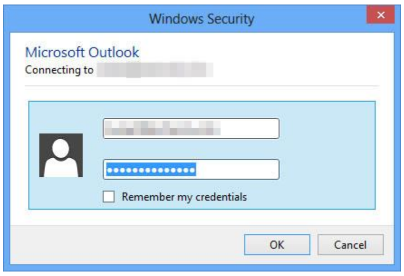
By using a mixture of upper and lower case letters, numbers or other characters your password will be harder to crack.

**DON’T USE:**

- Family members or pets names.
- Personal information like dates of birth, place names, addresses, favourite football team - these kind of details are usually easy to work out if you use social media
- Numerical or character sequences – 123456789, qwertyuiop, 11111111, abcdefgh the word “password” or phrases like “letmein” – not even by substituting numbers or characters – hackers already know to try “Pa$$w0rd!”

**Some other things to be aware of**
If for some reason you **do** have to change your password, remember the other places where you will need to change your password. For example:

- If you use 365 services (Word, Outlook, OneDrive, Yammer, etc.) on a phone then you will need to change the password on the apps.
- If you use the Outlook Client you may need to enter your new password and tick the box **remember my credentials** the first time you start Outlook after a password change.



Windows Security

Microsoft Outlook
Connecting to

□ Remember my credentials

- College Systems such as Columbus, Cintra, Tequios, P2P and so on have a separate password system – access to these systems is not affected by changes to your college account password. However you must change these password to include the guidelines set out in this document.
- Systems such as Moodle which use your college username and password to log in will allow access as before as long as you log in with your updated password.

- Password Managers are becoming popular, they allow you to store all your passwords (including non-College passwords) in a secure vault. They also generate hard to guess passwords can make them unique across all your services. The College encourages the use of Password Managers.

Security and Identity management are fast moving industries with quickly emerging technologies, this procedure will continue to be updated as new technologies or advice become available to the College. Only significant changes will be communicated to staff and students.

## FURTHER INFORMATION

If you need any help with this procedure, please contact the ICT Helpdesk:

**Email: ictservicedesk@glasgowkelvin.ac.uk**
**Service Desk:** http://ictservicedesk.glasgowkelvin.ac.uk:8080
**Extension No.:** 4585
**Telephone:** 0141 630 4585

**+++ END OF DOCUMENT+++**