UNIVERSITY OF
WEST LONDON

Password Policy

Responsibility of: IT Services
Approval Date: June 2018
Review Date: June 2020
Approved By: Vice Chancellor’s Executive

1 Introduction

1.1 Passwords are an essential part of securing important systems and data in the University of West London. Users of password protected systems must select, use, and protect strong passwords.

1.2 This policy applies to all users with accounts on University systems that are protected by a username and password.

2 Policy

2.1 Passwords must be kept confidential at all times and not disclosed to any other persons, including the IT Services team. You are responsible for any activity that is carried out using your user ID.

2.2 Passwords must not be written down anywhere that other people might be able to see or discover them. The IT Service Desk can advise on safe storage of passwords if this is required.

2.3 When choosing a password, you must select one that is strong, meeting these requirements:

- At least 10 characters long.
- Contains a mixture of upper and lower-case letters.
- Includes at least one number, punctuation mark or other special character.
- Chosen entirely at random, with no connection to you or the University.
- Not based on a single dictionary word.
- Does not include your name or username.

See the Appendix to this policy for guidance on choosing a strong but memorable password.

2.4 Changing your password regularly is not required, other than as set out in sections 2.5, 2.6, and 2.7.

2.5 If for any reason you suspect that your password has become known to any other person or has otherwise been compromised, you must change it as soon as possible and report your suspicions to the IT Service desk.

2.6 When you are first issued with an account, you will be given a temporary password. You must change this temporary password as soon as possible to a strong password you have selected, known only to you.

2.7 Sometimes IT Services will need to change your password for you, for example if you have forgotten it and are unable to use the self-service password reset. If this happens you must change this temporary password as soon as possible to a strong password you have selected, known only to you.

2.8 Some University systems may have additional password requirements, depending on the type of system, regulatory or contractual requirements, or the type of data they process. Follow the password guidance given by the administrators of those systems.

2.9 Do not reuse passwords or use the same password for multiple systems. In particular passwords used for University systems must never be used for systems outside the University.

Appendix – Guidance on Password Best Practice

To change your password, you should first register for self-service password resets at https://mysecurity.uwl.ac.uk/ Once registered you will be able to reset your password at any time by visiting https://mypassword.uwl.ac.uk

~

To choose a strong password, select three random words, for example by opening a book to a random page and picking any three words. Using mixed upper and lower case, combine the words using a punctuation mark or number as a separator. Some examples:

Time.Word.You SILENT-get-wish Open.Left.No

(Do not use any of these examples as your password!)

If you happen to pick three very short words, you might end up with a password that is too short; in that case simply pick a different three words.

For additional strength, you can simply add a fourth random word. The longer your password is, the more secure it is.

~

Below are some examples of bad passwords. Never use these or anything similar:

Sequences of numbers, like 1234567890 or 54321.

Single words, like football or password.

Simple keyboard patterns like qwerty or 1qa2ws3ed.

Dates such as 30071966 or a family member's birthday.

Short, common phrases like iloveyou or letmein.

Note that taking a bad password and making minor adjustments, such as adding a number or substituting zero for letter o, is not enough to make it into a good password. Use the three words method described above instead.

~

Be careful when you enter your password. Make sure no-one can see you typing it – this is called shoulder surfing. And be sure to only enter it into genuine UWL systems – be suspicious of any link received in an email that, when followed, asks for your username and password. Was it a genuine email or a phishing attempt?