UNIVERSITY OF WOLVERHAMPTON

PASSWORD POLICY

1 Introduction

1.1 Passwords are a critical aspect of our information and cyber security measures. They are our first line of defence.

1.2 This policy:

1.2.1 establishes guidelines on selecting strong passwords

1.2.2 provides for the protection of passwords, and

1.2.3 sets out how often passwords must be changed

1.2.4 sets out how often a password may be reused

2 Scope

2.1 This policy applies to all staff members of the University including employees, temporary and agency workers, interns, volunteers, apprentices and any other agents with access to the University's system. This includes all computer systems, laptops, tablets, personal devices and smart phones.

2.2 This policy applies to any device, whether University or personally owned, which is used for University purposes, whether on a regular or an ad-hoc basis.

2.3 This policy should be read in conjunction with the following:

2.3.1 Acceptable Use of IT Facilities Policy

2.3.2 IT Account Terms and Conditions

2.3.3 Encryption Policy

2.3.4 Information Security Policy

2.3.5 Data Protection Policy

2.3.6 Data Breach Policy

3 Using strong passwords

3.1 Your passwords must:

3.1.1 include a combination of both upper and lower case letters, symbols and numbers, depending on length

3.1.2 be at least 8 characters long (20+ characters is the recommended standard)

3.1.3 not be based on personal information (i.e. family names etc.)

3.2 To make your password even stronger, you may wish to adopt the following standards:

(a) For Passwords between 8-11 characters in length:

(i) requires mixed case letters, numbers and symbols;

(b) For Passwords 12-15 characters in length:

(i) requires mixed case letters and numbers;

(c) For Passwords 16-20 characters in length:

(i) requires mixed case letters ;

(d) For Passwords over 20+ characters in length:

(i) any characters you wish;

3.2.2 use letters which do not make up a word, i.e. it would not be found in a dictionary

3.2.3 avoid:

(a) using the University's name or any derivation

(b) word or number patterns (i.e. qwerty, 12345, abc123, etc.)

(c) any of the above backwards

3.2.4 Password Tips:

(a) Using a password of 16+ characters is considered the simplest password to input using hand-held devices as you merely need to change case level without any additional symbols or numbers, which is considered to make input simpler.

Password protection

3.3 Do not:

3.3.1 write your passwords down anywhere

3.3.2 share your password with anyone

3.3.3 insert your passwords into email messages or any other form of electronic communication

3.3.4 use the same password for work and personal accounts

3.3.5 use the 'remember me' or 'remember password' facility on websites or applications

4 Administrative passwords

4.1 Administration passwords for servers and databases require additional security features. The following security profile for administrative passwords is recommended:

(a) Administration rights for servers or project databases will be immediately removed when the member of staff leaves their role or terminates employment

(b) Administration passwords should have a minimum length of 12 characters

(c) Administration accounts will be reviewed every 12 months to ensure the accounts are still required and active

(d) Administrative passwords will change every 90 days

(e) Administrative passwords will not be displayed when input for authentication.

5 Changing passwords

5.1 All user passwords must be changed at least every 6 months

5.2 Users who have system administration rights must change their passwords at least every 6 months.

5.3 Password history shall be retained for a period of 3 x changes, re-use of the password is restricted whilst existing in the history

5.4 Users within the University premises or on University devices may change their password by pressing Ctrl+Alt+Delete

5.5 Users outside of the University may visit the University's Home Page, select "Staff", then click "Change your IT Password" from the "Quick Links" section

6 Expired Password

6.1 Users who fail to change their password within the prescribed time limits shall have their account disabled.

6.2 In order to regain access to an account, users shall contact IT Services (ext. 2000).

7 Automatic reminders

7.1 Users may receive an automatic reminder 10 days prior to the expiration of the current password.

7.2 All users should ensure that emails concerning the change of password are clearly recognisable as legitimate University of Wolverhampton correspondence. Should users be in doubt, they must at all times contact IT Services (ext. 2000).

7.3 An automatic reminder will never ask you to update your password via a direct external link.

8 Encryption of devices

8.1 The University of Wolverhampton employs a further means of improving account security by way of mandatory encryption of devices. This requires you to input a digital code each time you use a University laptop device (excluding shared Laptops). Desktops are encrypted but can be accessed without the need to input a device PIN.

8.2 Users are responsible for ensuring that all devices are appropriately encrypted in line with the University's Encryption Policy prior to its use for any University purposes. University data must not be stored on an unencrypted device, storage of University data in contravention of this requirement may result in disciplinary proceedings and a regulatory fine.

9 Responsibilities

9.1 All users have a responsibility for the security of their own passwords and for the reporting of actual or potential disclosures of own or other users' passwords in line with the University's Data Breach Policy.

10 Monitoring compliance with this policy

10.1 The Data Protection Officer is responsible for this policy.

10.2 All staff must be aware of and adhere to the policy. All staff will receive information on its requirements.

10.3 You may be liable to disciplinary action if you fail to comply with the provisions of this policy.

11 Review of our password policy

11.1 This policy is subject to annual review. We will provide information and/or training on any changes made.

VERSION:	**1**	**AUTHOR/ OWNER:**	**Office of the University Secretary**
Approved Date:	May 2018	**Approved By:**	(CMT)
Review Date:	May 2019		