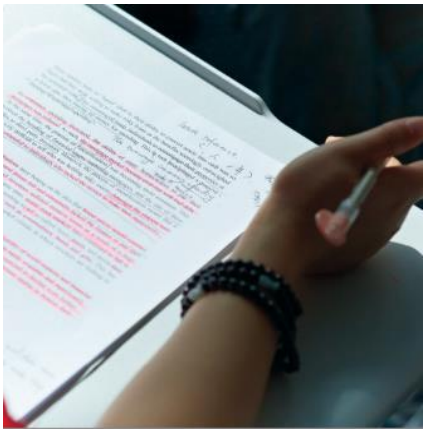
UNIVERSITY of BRADFORD

IT Services

Password Policy



UNIVERSITY of BRADFORD

Version control

Owner:	IT Director
Author:	IT Security Risk Manager
Approved by:	Executive Board
Date of approval of this version:	18 May 2023
Next review date:	As necessary, and not to exceed three years after approval date
Version number:	1.0
Applicable statutory, legal or national best practice requirements:	National Cyber Security Centre (NCSC) ISO 27001:2013 Information Security Management Standard UK General Data Protection Regulation (UK GDPR) Data Protection Act 2018
Equality impact assessment completion date:	31 January 2023
Data protection impact assessment completion date:	Not applicable

This document can only be considered valid when viewed via the University website. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one on the University website. Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

UNIVERSITY of BRADFORD

Contents:

1. Introduction

1.1 This document forms the password policy and guidance for staff, students and third parties.

1.2 The policy has been drawn from the controls referenced in the University's IT Acceptable use Policy and guidance from the National Cyber Security Centre. This is to ensure that passwords used to access computer resources are carefully chosen, kept, and updated in line with the University Acceptable standards.

1.3 The University's IT Acceptable Use Policy states that all users are responsible for all activity that takes place under their username and must not allow anyone else to access IT resources using their username and password. Users must therefore take all necessary steps to protect and maintain the security of their passwords, to ensure confidentiality, integrity, and availability of the University's resources.

1.4 This policy dictates the minimum that a user must do to conform to this requirement when selecting and updating a password.

1.5 The University uses 'single sign on' where possible so that a user can authenticate seamlessly against multiple services.

1.6 Core IT systems and services such as email and remote access will be protected by multi factor authentication (MFA).

1.7 All University IT systems use password authentication as a minimum.

2. Scope

2.1 This policy applies to students, staff, temporary workers, associates, and other workers at the University, including all personnel affiliated with third parties such as contractors / consultants, and emeritus users who have been provided with a University IT account.

2.2 This policy applies to standard users. Additional requirements for privileged users / administrators, and system specific accounts, are defined in a controls document approved and managed by the IT Services department.

3. Policy statements

3.1 All University users and third parties must:

- set a unique password for their University account
- not re-use the password
- not use their University password for any other services, whether personal or work / study related

3.2 All University users and third parties must protect their password and not share them with other users. The use of shared generic accounts will only be permitted following approval by IT Services, and in exceptional cases only.

3.3 Passwords shall be at least 12 characters in length, although longer passwords or passphrases are recommended.

3.4 Passwords must not contain the following:

- name or account username
- date of birth
- address (or any part of it)
- name of relatives or pets
- other personally identifiable information

3.5 If a University user knows or suspects that their password has been compromised, they must immediately notify IT Services, and change their password.

3.6 New passwords must not be the same as previously used passwords. Where possible, technical controls will be used to enforce this restriction.

3.7 A password change will be enforced without notice when in response to security incidents and emerging risks or where IT monitoring detects suspicious activity.

3.8 Passwords must not be based on commonly used passwords – for example, 'qwerty1234', 'pa55word1234' etc. Where possible, technical controls should be used to enforce this restriction.

3.9 Passphrases, including groups of random words are recommended as good strong password choices – for example, 'Mybr0th3r1sta11'.

4. Multi factor authentication (MFA)

4.1 MFA protects user accounts and information by combining a password with an added factor – this includes, but is not limited to, a smartphone authenticator app, a one-time password or pin (OTP), an SMS text code, and a hardware token / key.

4.2 All University users and third parties must enrol in University MFA processes, where they are deployed, to protect their account.

4.3 IT advice and guidance on password and MFA can be found on the IT Services intranet site.

5. Enforcement and sanctions

5.1 The University reserves the right to audit compliance with the policy from time to time. The breach of this policy shall be dealt with in accordance with the University's Disciplinary Policy.

6. Related policies and standards and documentation

6.1 IT Services Acceptable Use Policy

6.2 NCSC guidance on passwords

6.3 University guidance on passwords and multi factor authentication