BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891

# Password and Multifactor Authentication Policy

# Contents



| | | | |
|---|---|---|---|
| **Approved by:** | Digital Experience Steering Group | **Date first published:** | Apr-2024 |
| **Version:** | 1.0 | **Date updated:** | Apr-2024 |
| **Owner:** | Director of DTS | **Review Date:** | Apr-2029 |

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the University Secretariat.

# Purpose

1 In today's increasingly digital world information security and cyber vigilance is more important than ever. Both passwords and Multifactor Authentication (MFA) are security measure that help to bolster the protection of Buckinghamshire New University's (BNU) information assets.

2 Passwords are an important aspect of information security and are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the BNU entire network.

3 MFA requires users to provide two credentials in order to authenticate their identity and gain access to IT facilities. Rather than just asking for a username and password, MFA requires additional information (e.g. approving an authenticator app notification request) to log in, which adds an additional layer of security to your University account.

4 The purpose of this policy is to define the password and multifactor authentication requirements for accessing BNU IT systems and services from both on and off campus.

# Applicability and Scope

5 This policy applies to all University students, staff, partners, affiliates, contractors and third parties whether using a university issued or personally-owned devices to connect to the university's network and IT facilities.

6 All University IT systems must use password authentication as a minimum. The University uses Single-Sign-On (SSO) where possible so that a user can authenticate seamlessly against multiple services.

7 Recognising the limitations of passwords, where supported, all IT systems and services such as email, cloud storage, and remote access, will be additionally protected by MFA. This includes those systems supported by DTS as well as systems administered by other support departments and third-party providers.

# Passwords

8 Passwords must be kept confidential. Never share your password with anyone, including DTS. All passwords are to be treated as sensitive, confidential BNU information. DTS staff will never ask for full details of your password.

9 Passwords must not be written down anywhere that other people might be able to see or discover them or stored in a file on ANY computer system (including phones or similar devices whether they are University or personally owned) without encryption.

10 You are responsible for any activity that is carried out using your account so to help keep your password secure you may wish to use a password manager app that can safely store a variety of passwords and make them easy to reference when you need to. Any use of password managers must follow the advice provided by the National Cyber Security Centre (NCSC).

11 When you are first issued with an account you will be given a password which you must change as soon as possible to a strong password known only to you. To change your password, you should first register for self-service password reset by following the link on the IT web pages. Once registered you will be able to reset your password at any time.

12 You are required to change your password every 12 months. You will receive regular reminders to change your password before the expiry date. When your password expires you will lose access to IT systems and services.

13 If you believe your password has been compromised or made available to others, you must immediately change it and notify the IT Service Desk.

14 Passwords must not be inserted into e-mail messages or other forms of electronic communication and must not be stored or transmitted in clear text (unencrypted).

15 Do not use the same password for your BNU accounts as for other non- University access (e.g., personal e-mail, on-line banking, and social media).

16 Guidance to set a good password can be found on the DTS Self-Service Portal

## Multifactor Authentication

17 All users must enrol a device with the BNU MFA service to get access to University systems and services. If multifactor authentication is required for a system, failure to register a suitable device may mean that you are unable to authenticate and use the system.

18 You must not share or disclose the MFA one-time codes with anyone else, including DTS. DTS staff will never ask for your MFA details or one-time codes.

19 If you have access to a University issued mobile phone or tablet the authenticator app must be used as the default multifactor authentication method.

20 If your registered devices are lost, stolen, infected with malware or you have reason to suspect your BNU issued IT Credentials such as user name and/or password have been compromised, you must notify the IT Service Desk without undue delay.

21 If you have any concerns about enrolling for MFA, contact the IT Service Desk in the first instance.

## Exclusions or Special Circumstances

22 There may be situations in which a user has a legitimate need to access BNU IT facilities outside the scope of this policy. The Director of DTS or their nominated representative may approve, in advance, exception requests based on balancing the benefit versus the risk to the University. Exception requests must be made through the IT Service Desk.

## Enforcement

23 Any actual or suspected breach of this policy must be reported to the Director of DTS via the IT Service Desk. The Director of DTS will take appropriate action and inform the relevant internal and external authorities.

24 Failure to comply with this policy may result in disciplinary action in accordance with the relevant process.

# Key Relevant Documents

25 This policy should be read and understood in the context of other Buckinghamshire New University Policies which together form the Information Security framework. Key documents include:

- Acceptable Use Policy
- Data Protection Policy
- Information Security Policy

# Table of Definitions

| | |
|---|---|
| IT Facilities | Hardware, software, data, network access, third party services, online services or IT credentials provided or arranged by Buckinghamshire New University. |
| IT Credentials | Your institutional login, or any other token (email address, smartcard, dongle) issued by the University to identify yourself when using IT facilities. |
| Multi-factor Authentication (MFA) | The use of two different components to verify a user's claimed identity. Also known as two-factor authentication (2FA). |
| Staff | Staff are salaried members of the University or contracted individually by the University to provide a service. |
| Student | A person pursuing any course of study in the University. |
| University information | Includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media |

# Appendix: Equality Impact Assessment

As a university, we are committed to enhancing equality, diversity and inclusion (EDI). We have a legal (Equality Act 2010) and ethical obligation to ensure our policies, systems and processes are fair, inclusive and ensure every member of the BNU community can thrive.

Whilst we all have protected characteristics, we know there are certain characteristics and communities that are marginalised and underrepresented in Higher Education and the workplace. These are: different ethnicities (including Gypsy, Roma, Traveller, Showmen and Boaters, migrants, refugees and asylum seekers) Disabled individuals; neurodiverse individuals; pregnancy (including maternity and paternity impact); the LGBT+ community; carers; people of different faiths; people impacted by menopause and individuals from a range of backgrounds including: socio-economic disadvantage, homeless, alcohol and/or substance misuse, people experiencing domestic and/or sexual violence, ex-armed forces, looked after children and care leavers. We also know individuals have multiple intersectional experiences and different points in their lives and careers.

1. **With reference to the above characteristics, in what ways does this policy enhance equality and the access of opportunity at BNU?**

   The policy applies to all users in the same way therefore has the potential to impact all groups however there may be a positive impact on groups who need to access systems and services outside of standard working hours.

2. **In what ways does the policy adversely impact individuals from marginalised and underrepresented communities?**

   The policy applies to all users in the same way therefore has the protentional to impact all groups however there may be the greatest impact on the protected characteristic of disability.

   Users in this category may need to make use of assistive technologies when performing MFA, for example, screen reader, zoom, Face ID or voice control. They may also choose to use SMS text message or voice call for authentication. The recommended MFA smartphone app is compatible with accessibility features available on Apple and Android smartphones (e.g. screen-reader) and additional MFA methods (SMS text message and voice call) are available to users who are unable to use apps.

   It is also noted that people of different ages will have mixed technical ability and to that end, additional support will be available for those users who struggle to change their password or configure MFA.

3. **How does this proposal work towards achieving the BNU Equality Objectives as outlined in the Equality Strategy 2023-2028? Please signpost objectives and actions in the BNU Equality Strategy.**

   This policy is a factual and procedural document, providing details on how the University monitors the use of computers and network by staff, students and other users. It addresses compliance with laws and regulations and the need to protect the University's information, balanced with the need to protect the rights of learners, staff and partners.

**Signed:**
**Name:**
**Date:**

**High Wycombe Campus**
Queen Alexandra Road
High Wycombe
Buckinghamshire
HP11 2JZ

**Aylesbury Campus**
59 Walton Street
Aylesbury
Buckinghamshire
HP21 7QG

**Uxbridge Campus**
106 Oxford Road
Uxbridge
Middlesex
UB8 1NA

**BNU based at Pinewood Studios**

Pinewood Studios
Pinewood Road
Iver Heath
Buckinghamshire
SL0 0NH

**Missenden Abbey**
London Road
Great Missenden
Buckinghamshire
HP16 0BD

Telephone: 01494 522 141

BucksNewUni

BucksNewUni

BucksNewUni

BucksNewUniversity

If you have any queries about this policy, please contact the School or Directorate responsible for the policy