www.rbwm.gov.uk

Royal Borough of Windsor & Maidenhead

Royal Borough Windsor & Maidenhead

Password Construction Guidelines

June 2022

“Building a borough for everyone – where residents and businesses grow, with opportunities for all”

Our vision is underpinned by six priorities:

Healthy, skilled and independent residents
Growing economy, affordable housing
Safe and vibrant communities
Attractive and well-connected borough
An excellent customer experience
Well-managed resources delivering value for money

Contents

Frequently used acronyms

IT	Information Technology
RBWM	Royal Borough of Windsor & Maidenhead

1 PURPOSE

1.1 The purpose of this guideline is to provide best practice for the creation of strong passwords.

1.2 Passwords are an important aspect of computer security and a critical component of information security. A poorly constructed password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems and can compromise our entire infrastructure.

1.3 All staff, including contractors and vendors with access to the Royal Borough of Windsor and Maidenhead systems, are responsible for taking the appropriate steps, as outlined in the Password Policy to secure their usernames and passwords and follow this guideline with best practices for creating secure passwords.

2 SCOPE

2.1 This Password Construction guideline outlines best practise guidelines relating to password construction and applies to all RBWM employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties.

2.2 This guideline applies to passwords created for all RBWM systems including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

3 APPLICABILITY

3.1 This guideline applies to all council employees and RBWM Councillors. The Password Policy also applies to contractors, temporary, agency staff, partners and others working in a similar capacity that can access, manage, or process information assets of the council. They are also accountable for understanding and adhering to the guidance contained in this guideline and any applicable supporting policies and procedures. All applicable persons listed above are referred to as ‘users’ in this guideline.

4 AUTHORISATION

4.1 Only authorised persons should have access to council assets and systems or accessing the council IT or mobile network. Any user that deliberately or inadvertently accesses the council IT or mobile network or systems unauthorised, will be in breach of the Password Policy.

4.2 For any council business:

4.2.1. Users accessing council IT facilities must comply with all council policies and procedures.

4.2.2. Managers and Team Leaders must ensure their staff comply with the Password Policy and provide advice to them.

4.2.3. Managers and Team Leaders must ensure security incidents are raised in response to IT access security concerns or security breaches as covered in the Reporting Security Incidents Policy.

4.2.4. IT Services provide technical solutions to support different IT access security levels, depending on the sensitivity and value of the data accessed. Administer, control and monitor access to IT facilities and systems.

4.2.5. IT Services ensure that privileged and systems administrator access is strictly controlled based upon a valid business justification and specific job requirements as approved by the user's line managers.

5 POLICY COMPLIANCE

5.1 Compliance Measurement

5.1.1. All users must comply with the Password Policy.
5.1.2. The IT Support will verify compliance to the Password Policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1.3. If you do not understand the implications of the Password Policy, how it may apply to you, or your security responsibilities when working with the council, please seek advice in advance from your line-manager or contact the council's Data Protection Officer at dpo@rbwm.gov.uk.

5.2 Exceptions

5.2.1. Any exception to the Password Policy must be approved by the IT Senior Management Team in advance.

5.3 Non-Compliance

5.3.1. Any breach of this policy may be subject to disciplinary action under the council’s disciplinary procedures, up to and including dismissal. In circumstances where it is believed that a criminal offence has been committed the matter may be reported to the Police.

6 STATEMENT OF GUIDELINES

6.1 The Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 16 (sixteen) characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” or “block curious-sunny-leaves”. Passphrases are easy to remember and type.

6.2 Every work account should have a different, unique password. Whenever possible, also enable the use of multi-factor authentication.

6.3 Poor, or weak, passwords have the following characteristics:

6.3.1. Contain less than 10 (ten) characters.

6.3.2. Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

6.3.3. Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

6.3.4. Are some version of “Welcome123” “Password123” “Changeme123” “Monday123”

7 UNIQUE USERNAMES / IDENTIFIERS & PASSWORD / PASSPHRASES

7.1 It is important to use different passwords for different services. This way, if one service is compromised, your credentials cannot be used to access information from other services.

7.2 At RBWM we implement unique usernames. Users are not allowed to share usernames, if they do, they will also share passwords, which means the credentials are no longer secret.

7.3 It is always of utmost importance to protect User identifiers (usernames) and passwords. Never reveal your user credentials; usernames, IT access codes, passwords, or passphrases to anyone, unless requested by RBWM IT Service support. The password should be updated by the individual after the support has been completed.

7.4 Do not allow others to see you enter the characters or numbers you input when entering your user identifier, access code or password.

7.5 Avoid writing down your user identifier(s), IT access codes or passwords. If you need to write them down keep them out of sight, preferably locked away.

8 PASSPHRASES

8.1 The use of passphrases instead of passwords are encouraged to increase security.

8.2 While passwords are usually strings of around 10 letters, numbers, and symbols, (e.g., "2GetherForever1985!"), passphrases are groups of words with spaces in between, e.g., "We Never Drive Past the M23 Service Station!"

8.3 A passphrase can contain symbols, upper- and lower-case letters, spaces and does not have to make sense grammatically.

8.4 Passphrases are generally easier to remember, but harder to crack than passwords.

Passphrase and Password comparison:

Passphrases	**Passwords**
Contain **words and spaces** and can also contain strings of upper-/lower-case letters, numbers, and symbols	Contain strings of upper-/lower-case **letters**, **numbers**, and **symbols**
Easy to remember passphrases of up to **127 characters** long	It's difficult to remember passwords > 10 characters
Extremely difficult to crack a long passphrase	Passwords < 10-character can be cracked between 1min – 4hrs

9 PASSWORD COMPLEXITY RULES:

9.1 The Passwords/Passphrases must be at least 16 (sixteen) characters.

9.2 The password must contain characters from at least three of the following categories:

9.2.1. Uppercase (A,B,C…Z),

9.2.2. Lowercase letters (a,b,c…z),

9.2.3. Numbers (0,1,2…9), or

9.2.4. Special characters / symbols (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

9.3 The password cannot contain any 3 (three) consecutive characters that are part of your username / identifier.

9.4 Administrator passwords should include ALT characters in the 0128–0159 range to enhance the complexity of a password. (ALT characters outside of this

range can represent standard alphanumeric characters that would not add additional complexity to the password.).

APPENDICES

RELATED STANDARDS, POLICIES AND PROCEDURES

- Password Policy.
- Reporting Security Incidents Policy

Document name	Password Construction Guidelines
Document author	Infrastructure security manager
Document owner	**Head of HR, Corporate Projects and IT**
Accessibility	
File location	
Date destruction	
Circulation restrictions	

How this document was created

Version	**Date**	**Author**
Version 1	25/06/2020	Infrastructure security manager
Version 2	23/10/2022	Strategic Lead, IT Services
Version 3		

Review date: 22/10/2024