Password Policy Template for UK SMEs

Executive Summary

- Reused and weak passwords are among the biggest threats to the security of small and medium enterprises (SMEs) in the UK.
- Implementing a straightforward, enforceable password policy greatly minimises the risk of cyber attacks.
- The length of a password is more significant than its complexity (such as the use of special characters).
- Multi-factor authentication (MFA) is an integral part of any effective security system, rather than an optional one.
- There are gaps in accountability and security associated with the use of shared accounts.
- Using a password manager rather than notebooks or spreadsheets is more secure.
- There are regulatory requirements imposed on SME organisations as per the General Data Protection Regulation (GDPR), which include the use of appropriate technical measures, and passwords are a technical measure.
- SMEs can develop a secure password policy using free or nearly free solutions, rather than

Who This Guide Is For

This guide is intended for the following groups:

- Businesses with less than 50 staff, in the UK.
- Owner driven companies.
- HR and Office Managers.
- IT Administrators.
- Decision-makers who are not technical.

Why a Password Policy Matters

- The majority of cyber attacks start with stolen credentials.
- The majority of breaches stem from phishing and reused passwords.
- Examples of breaches include:
- 8 person consulting company with a hacked Microsoft 365 account.
- One login for 2 different services (Microsoft 365 and property management).
- The GDPR Article 32 requires "appropriate technical measures".
- The ICO expects security controls to be proportionate to the risks associated with a breach occurring.
- Cyber Insurance companies increasingly require MFA and strong passwords as an essential part of their policies.

Common Password Mistakes & Threats

A place to explain passwords simply includes the following:

- Weak passwords (example: "Password123").
- Reused passwords.
- Written passwords on paper.
- Shared logins between employees.
- Failing to remove login access for terminated employees.
- Phishing emails that trick users into entering their passwords.
- Automated Credential stuffing (Attackers using previously stolen usernames & passwords).

Key Policy Components

1. Minimum Password Length

What is it: The minimal length that can be used for passwords.

What is the importance of this: The longer the password is, the exponentially more difficult it is to crack them.

How do we implement this:

- **Minimum** is to have 12 characters
- **Recommended** is to have 14-16 characters (encourage pass phrases)

  The best is to have no upper limit only have a lower limit
- **Typical mistakes:** Still have an 8-10 character requirement
- **Fast Wins:** Change policy to require minimum of 14 characters; discuss pass phrase examples (Example: BlueHorseBatteryStaple2026!)

2. Password Complexity

What is it: Rules defining what types of characters (upper case, lower case, numbers, symbols) can be included in passwords.

What is the importance of this: By increasing character type usage, the total number of possible passwords increases significantly. However, if there are too many restrictions on allowable passwords, users are likely to reuse them.

How do we implement this:

- **Minimum:** no complexity rules (longevity is better)
- **Recommended:** Ban the use of easily guessable words & require at least one number/symbol in the password
- **Best:** Allow any character through; block the bottom 10,000 most used passwords
- **Fast Wins:** Remove forced complexity from passwords; block the common password examples "Password1", "Company2026".

3. Password Rotation / Change Frequency

What it is: The frequency with which users are required to change their existing passwords.

What is the importance of this: Forcing users to change their passwords creates an opportunity for them to create weaker possible passwords than they would have used previously.

How do we implement this:

- **Minimum** is No forced password change (NCSC & NIST guidance)
- **Recommended:** Change Password only when either: Compromised or suspected.
- **Best:** Completely remove password expiry
- **Fast Wins:** Turn off 90-day password change requirement in Microsoft 365 / Google Workspace.

4. Preventing Reusing Passwords

What it does: Prevent using previously used passwords.

Why is this important? Prevents patterns such as "Password1 → Password2."

How to implement:

- **Minimum:** Keep track of 5-10 old passwords
- **Better:** Block 24 most recent previous passwords (Microsoft default)
- **Best:** Incorporate lists of breached passwords (HaveIBeenPwned API)
- **Quick win:** Enable "you cannot reuse previous passwords" in your directory

5. Lock Account After 3 Failed Attempts

What it does: Locks your account for a short period after a wrong attempt.

Why is this important? Prevents guessing by brute-force attack

How to implement:

- **Minimum:** Lockout after 10 failed attempts for 15 minutes.
- **Better:** Lockout after 5 failed attempts for 30 minutes.
- **Best:** Employ progressive delays for accessing accounts (e.g. 1st attempt 10 minutes, 2nd attempt 20 minutes, etc.), notify System Administrator after 3 failed attempts.
- **Quick win:** Set lockouts to 5-10 attempts in your environment.

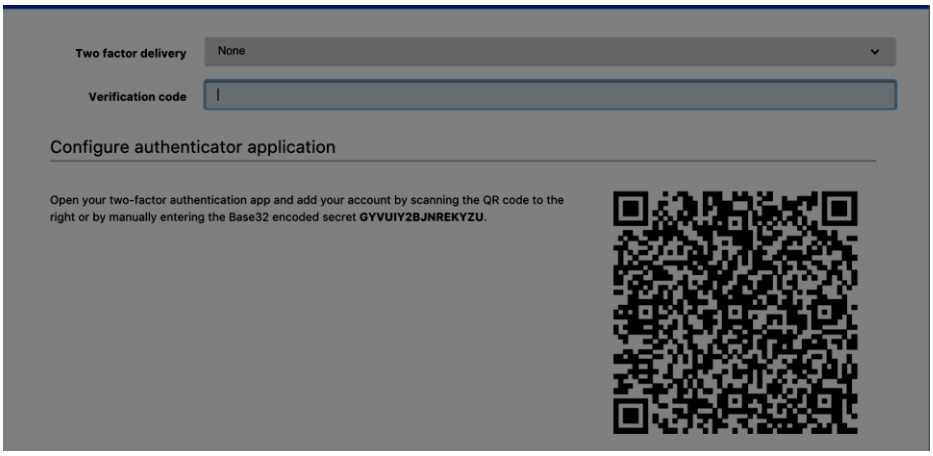
Multi-Factor Authentication (MFA) & Secure Logins

What does it do: A second verification step (via different methods such as phone code or authenticator app) is required after entering your password.

Why it is Important: Prevents approximately 99.9% of automated credential attacks. (Microsoft data)

How to Implement:

- **Minimum:** Require MFA for administrative and privileged accounts.
- **Better:** Require MFA for all employees with email and/or access to Cloud storage/CRM.
- **Best:** Enforce MFA for all employees with email and/or access to Cloud storage/CRM, using phishing resistant methods (FIDO2 Key, Authenticator push notification).
- **Quick win:** Turn on MFA for Microsoft 365 and Google Workspace NOW (should take ~15 minutes to enable throughout your entire environment).



Two factor delivery None

Verification code

Configure authenticator application

Open your two-factor authentication app and add your account by scanning the QR code to the right or by manually entering the Base32 encoded secret **GYVUIY2BJNREKYZU**.

Password Storage and Sharing Practices

- No Shared/ Generic Accounts
- All Staff Use a Password Manager
- Revocation of Access After an Employee Leaves
- Do Not Store Passwords in Spreadsheets

GDPR and UK Data Protection Compliance Considerations

- Responsibilities of Data Controller
- Technical Security Measures Must be Practical
- Document you Policy
- Submit a Breach Report to the ICO if a Passwords are Compromised
- Must Comply with Cyber Essentials

30-Day Implementation Plan with Checklist

Week 1: Foundational Activities

- Prepare Draft of Security Policy
- Determine Required Minimum Length
- Identify Unknown Admin Accounts

Week 2: Security Enhancements

- Implement MFA Where Possible
- Deploy a Password Manager
- Eliminate Shared Accounts

Week 3: Training and Audit

- Conduct Employee Security Awareness Training
- Conduct Phishing Test
- Review Access and Permissions

Week 4: Documentation and Review:

- Include Policy in Employee Handbook
- Confirm that security policy complies with the GDPR
- Schedule Annual Review of Security Policy

FAQ

➢ **What length do you require for your passwords?**

As a minimum, you should use a minimum of 14 characters, however, a long memorable passphrase is preferred.

➢ **Is there any continuing need for complexity?**

The length of the password is more important than forcing complexity; however, if possible block common passwords, and require at least one number and symbol.

➢ **How frequently do you want your passwords to be changed?**

All passwords should only be changed if compromised or suspected to be compromised and should not be changed at regular intervals.

- **Must multi-factor authentication (MFA) be used?**

It is a requirement, and it is required for all email, cloud and admin accounts.

- **Is a password manager safe?**

Yes, but reputable password managers are safer than storing passwords in a spreadsheet, notebook or reusing passwords.

- **Should all staff share their login information?**

No, all employees will use their own logon credentials.

- **What should be done if someone has lost their password?**

Follow the secure account reset process through IT or your system administrator, and verify identity prior to resetting password.

- **Does this requirement exist under the General Data Protection Regulation (GDPR)?**

Yes, the United Kingdom General Data Protection Regulation (UK GDPR) contains a principle regarding appropriate technical measures being used, and strong password requirements form part of that principle.

- **Do you have to have MFA to have Cyber Essentials?**

Cyber Essentials mandates multi-factor authentication (MFA) to be utilised for administrative users and/or for remote/cloud access.

- **What is a minimum safe setup?**

A minimum character length of 14, Use of Multi-Factor Authentication for all users, No shared accounts, and the use of a password manager.

About This Guide

This guidance and password policy have been developed by **Computer Support Centre,** based out of the UK. They offer IT support and cybersecurity consultancy services to SMEs (small medium enterprises) in the UK (1-50 employees) to help them establish clear, but affordable, measures to protect against cybersecurity and/or information risk, without too much unnecessary complication. They have written the guidance using a combination of current recommendations from the UK's National Cyber Security Centre (NCSC), guidance from the Information Commissioner's Office (ICO), internal best practices for Microsoft and Google, and their real experiences supporting UK SMEs between 2025 and 2026. The intent is to provide simple, non-technical guidance that is easily understood and actionable by all business owners and managers. They also assist businesses with the setup of both their password policies, deploying MFA solutions, establishing a password manager, training their staff on their use, and creating documentation in accordance with GDPR. If you are interested in a free review of your current password settings, or need assistance in customising and implementing this policy, please do not hesitate to reach out to us we would be pleased to have a brief informal discussion with you.

Conclusion

The UK's small businesses can protect their organisation's customer data, staff accounts and business systems with a strong yet simple password policy, which is one of the most effective methods of safeguarding their data from cyber attacks. A focus on using longer passphrases or phrases, mandatory use of multi-factor authentication (MFA), the removal of a requirement for regular, monthly password changes and safe storage of their passwords will reduce the chances of credential attack significantly, without causing daily work frustrations. Start this week with small, practical steps: enable MFA for all employees and create a new minimum length for passwords of 14 characters; complete a phased rollout of the full policy over the next 30 days. These actions reinforce your compliance with UK GDPR, demonstrating to your customers, regulators and insurers that you take data protection seriously and providing your business with greater resilience and peace of mind.