

Password Policy

v1.1 · Updated Jul 2026 · Reviewed Jun 2026 · Next review Jun 2027

Owner: Andrew James (CEO)

1. PURPOSE

This policy defines password requirements for all Halved Limited systems to protect against unauthorised access and meet Cyber Essentials requirements.

2. SCOPE

This policy applies to all passwords used to access:

- Halved email accounts (Microsoft 365)
- Cloud services (Azure, GitHub, MongoDB Atlas, Cloudflare, Xero, etc.)
- macOS user accounts
- Any other systems containing organisational data

Passwords that students and school staff set on the Halved platform itself are not covered by the scope above. They are governed separately by Section 9.

3. PASSWORD REQUIREMENTS

3.1 Minimum Password Standards

All passwords must meet the following minimum requirements:

- Minimum length: 10 characters
- No maximum length restriction
- Complexity: Use a passphrase (three or more random words) OR a mix of upper/lowercase letters, numbers, and symbols
- Uniqueness: Each system must have a unique password - never reuse passwords across services

3.2 Multi-Factor Authentication (MFA)

- MFA is required on all systems that offer it
- **Preferred MFA method:** Authenticator app (Microsoft Authenticator, Google Authenticator, or similar)
- **Acceptable MFA method:** SMS codes (where authenticator app is not available)
- **Not acceptable:** Email-based MFA does not count as true MFA

3.3 Password Management Requirement

All users must:

- Use a password manager to store passwords securely
- **Recommended password managers:** 1Password, Bitwarden, or macOS Keychain
- Never store passwords in plain text (documents, spreadsheets, notes apps)
- Never share passwords via email, Slack, or messaging

3.4 Admin Account Passwords

Administrative accounts require additional security:

Minimum length: 12 characters (must be different from standard account passwords)

MFA: Mandatory on all admin accounts

Uniqueness: Admin account passwords must be completely different from standard account passwords

4. PASSWORD CREATION GUIDANCE

4.1 Creating Strong Passwords

Good approaches:

- **Three random words:** CorrectHorseBatteryStaple
- **Passphrases:** ILove2DrinkCoffeeInTheMorning!
- **Password manager generated:** Let your password manager create a random strong password

Avoid:

- **Common patterns:** Password123, CompanyName2026
- **Personal information:** birthdays, names, addresses
- **Keyboard patterns:** qwerty123, asdfgh
- **Dictionary words on their own:** elephant (too weak without additional characters)

4.2 Password Expiry

- **No forced password changes:** Passwords do not expire on a schedule
- **Change immediately if:** You suspect your password has been compromised
- **Change immediately if:** A service reports a breach

5. COMPROMISED PASSWORDS

If you suspect your password has been compromised:

- **Report immediately:** Notify the CEO (Andrew James) within 1 hour
- **Change the password immediately on the affected account**
- **Check for reuse:** If you reused the password elsewhere, change it on all systems
- **Re-enrol MFA** if MFA may have been compromised
- **Monitor account activity** for unusual behaviour

6. NEW USER ONBOARDING

When a new team member joins:

- They are provided with this Password Policy during onboarding
- They set up a password manager before accessing any Halved systems
- They enable MFA on all accounts during first login
- CEO verifies MFA is enabled before granting access to sensitive systems

7. COMPLIANCE

Failure to comply with this policy may result in:

- Account suspension
- Disciplinary action
- Cyber Essentials certification failure

8. TRAINING

All users receive password security training:

- During onboarding (new users)
- Annually (refresher for existing users)
- After any security incident

9. PLATFORM-USER PASSWORDS (HALVED PRODUCT)

Sections 1 to 8 of this policy concern Halved's corporate systems, meaning the accounts staff use to run the company, such as Microsoft 365, Azure, GitHub and MongoDB Atlas. This section is separate. It governs passwords set by end users of the Halved platform, meaning students and school staff, through account setup, password reset and the in-app change-password form. The corporate requirements in Sections 1 to 8 do not apply to platform users, and the requirements in this section do not apply to corporate systems. Both scopes are stated explicitly so that the two are not read as one.

Where a school uses single sign-on with its own identity provider, Halved does not set or store a platform password for those users, and their passwords remain governed by the school's own policy. The requirements below apply only where Halved sets the password.

9.1 Minimum Requirements

The following are enforced on the server, on every route that sets or changes a platform password. Any check performed in the browser exists only to give the user a helpful message and is not the control.

- Students: a minimum of 8 characters, together with a common-password deny-list.

- Staff, meaning teachers, safeguarding leads, school administrators and Halved administrators: a minimum of 12 characters, together with a common-password deny-list.
- The deny-list is the NCSC “Top 100,000 passwords” list, published by the National Cyber Security Centre together with Have I Been Pwned. A password that appears on the list is rejected, and the comparison ignores letter case. The deny-list applies to every platform user, staff included, because length and commonness are independent risks and a long password can still be a common one.
- Platform passwords are stored only as salted bcrypt hashes. Halved does not store or log a plaintext platform password.

9.2 Cyber Essentials Alignment

Cyber Essentials requires, for accounts protected by a password alone, either a minimum length of 12 characters, or a minimum of 8 characters supported by a deny-list of common passwords. The student requirement meets the second route. The staff requirement meets the first route, with the deny-list added as a further layer. The higher bar for staff reflects their broader access to safeguarding data, to other users’ records and to administrative functions.

APPROVED BY:

Andrew James, CEO Halved Limited Date: 4th June 2026

Section 9 (Platform-user passwords) added and approved: 14th July 2026

Questions about data protection? dataprivacy@halved.io

Website halved.io · students log in at my.halved.io

Halved Limited · registered in England and Wales, company number 15261677