PASSWORD POLICY

Date of approval by the Trust Board	**25 March 2026**
Review cycle	**2 years**

1. PURPOSE

This policy is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

2. SCOPE

This policy applies to passwords for the use of all ICT services administered by Alternative Learning Trust ('the Trust') schools, including services provided under contract for the Trust. This policy does not apply to privileged accounts such as network and system service accounts, which do not belong to a nominated individual but are necessary for the automated operation of the network, applications and connected services.

3. POLICY STATEMENT

The information system resources are assets important to the Trust's business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. It is the school's policy that appropriate access control measures are implemented to protect its information system resources against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

Passwords are a key element of access control and require effective management to ensure that the school's ICT assets are not compromised by unauthorised access.

4. POLICY OBJECTIVES

The objectives of this policy regarding the protection of information system resources against unauthorised access are to:

- Minimise the threat of accidental, unauthorised, or inappropriate access to electronic information owned by the Trust or temporarily entrusted to it.
- Minimise the network exposure, which may result in a compromise of network integrity, availability, and confidentiality of information system resources.
- Minimise reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality.
- Raise awareness of the factors which either weaken or strengthen passwords to ensure that passwords of an appropriate strength are in use.

5. POLICY OVERVIEW

This policy sets out the rules, requirements and guidelines covering the management of passwords.

Passwords are important because they provide entry to the Trust's ICT resources.

Passwords play an important role in the defence against malicious misuse of these resources. Any misuse of passwords could result in the confidentiality, integrity or availability of vital information being compromised or the Trust being held responsible for illegal activities.

6. POLICY REQUIREMENTS

Responsibilities

- All users are responsible for ensuring that this policy is complied with.
- All users are responsible for maintaining Password security in accordance with this policy in all their activities.
- Any user who for any reason has gained temporary or permanent knowledge or use of a password relating to any part of an information system for which they do not normally have access should identify this to ICT contact immediately, so that the situation can be rectified.

7. PASSWORD CHARACTERISTICS

Passwords are used for various purposes; best practice dictates that user passwords should be described as either 'complex' or 'strong'.

Strong passwords have the following characteristics:

- Contain both upper and lower-case characters (e.g., a-z, A-Z).
- Have digits or punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./).
- Are at least eight alphanumeric characters long for normal user accounts.

NCSC PASSWORD RECOMMENDATION

Your email password should be strong and different from all your other passwords. Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.

Do not use words that can be guessed (for example, your pet's name). You can include numbers and symbols if needed; for example, "Hippo!PizzaRocket1".

Turn on Multi-Factor Authentication (MFA) to instantly upgrade your email security. MFA works by requiring an extra piece of information to prove your identity before granting access—such as entering a unique code sent to your phone whenever you sign in from an unfamiliar device or attempt to change your password.

You **will not** be asked for this every time you check your email.

8. PASSWORD HISTORY

Passwords should not be reused. A password should not be the same as the one used during the past five changes.

9. PASSWORD EXPIRY

- Student passwords do not expire; however, any student who needs their network login password changed can contact the ICT contact.

10. PASSWORD SECURITY

- The purpose of passwords is to protect the confidentiality and integrity of Trust IT facilities and assets. The combination of a particular username and password also provides an audit trail identifying which authorised user accessed a resource at a particular time.

- IT Services will disable any accounts identified as having shared passwords and makes the following recommendations to users as password best practices.
- Passwords must not be shared with anyone, including IT Services. All passwords are to be treated as sensitive and confidential information.
- Two factor authentications for Office 365 will be implemented for all staff and Trustees by September 2026 and will be used thereafter. Training will be arranged to support implementation.
- Three failed login attempts allowed before an account is temporarily locked to prevent brute-force attacks.
- IT-issued initial passwords must be changed by the user upon their first login.
- IT must verify a user's identity before granting a remote password reset request.

11. USERS ARE EXPECTED TO OBSERVE THE FOLLOWING:

- Do not e-mail or otherwise communicate your password to anyone.
- Do not reveal a password over the phone to anyone.
- Do not write a password down or store it on your computer in a format readable by others.
- Do not hint at the format of a password (e.g. “my family name”).
- Do not reveal a password on questionnaires or security forms.
- Do not use the “Remember Password” feature of applications and websites.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on leave.
- Do not include personal details which may be readily known to others (e.g. your partner’s name, your birthday, names of pets, and similar).
- Do not use common sequences of numbers or letters (e.g. 12345678 or qwerty, etc.).
- When leaving the desk to ensure the user ‘logs off’ the computer or if the computer is not shared with other users that it is ‘locked’.

12. REPORTING SECURITY INCIDENTS

All security incidents, including actual or potential unauthorised access to the School’s IT systems, should be reported immediately to the IT services team.

These incidents include occasions when:

- A password may have been accidentally revealed.
- It is suspected that access has been gained to a system by an unauthorised person.
- In addition to reporting a suspected breach, users must as a matter of urgency take immediate action and change their password.

13. DISIPLINARY PROCESS

The Trust (and therefore any constituent school) reserves the right to audit compliance with the policy from time to time. Any disciplinary action arising from breach of this policy shall be taken in accordance with the Trust’s Disciplinary Policy.

14. DEVIATIONS FROM POLICY

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation from or non-compliance with this policy shall be reported to the ICT Systems Co-ordinator in the first instance.

Person responsible for reviewing this policy:

Deputy CEO/Director of School Improvement