Unique Policy Number: 28.1

Password Policy

The Children's Endeavour Trust comprises:

Abbot's Hall Community Primary School
Bosmere Community Primary School
Broke Hall Community Primary School
Chilton Community Primary School
Combs Ford Primary School
Freeman Community Primary School
Springfield Junior School
Whitehouse Community Primary School

Document Control

Version	*Date*	*Author*	*Comments*
Issue 1	**July 2024**	**KW**	*New policy*
	Nov 2025	**KW**	*Readopted*

Owner: DPO
Approver: Trust Board
Statutory Policy: Yes
Review Cycle: 1 year
Approval date: 18th December 2025

Policy Contents

1. Introduction and Aims

The Children's Endeavour Trust and its schools (collectively referred as "CET" or "Trust") is committed to protecting the rights and freedom of all individuals in relation to the processing of their data.

This policy has been created to help enforce data protection recommendations with guidance from the National Cyber Security Centre (NCSC). and to minimise the risk of IT security incidents and data breaches in relation to all personal or sensitive data.

A safe and secure password policy is essential if the above is to be established and will apply to all ICT infrastructure within the Trust and social media accounts.

2. Objectives

The objectives of this policy with regard to the protection of information system resources against unauthorised access is 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; and
- Raise awareness of the factors which either weaken or strengthen passwords to ensure that passwords of an appropriate strength are in use.

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.

3. Responsibility

The Trust and each school's IT staff and provider will be responsible for ensuring that all ICT Infrastructure is safe and secure as is reasonably possible within their school.

This Password Policy is to ensure

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission

All users within the Trust provided with their own user accounts will have responsibility for the security of their username and password, they must not allow other users to access the systems using their log on details. Please refer to the Trust's Acceptable Use Policy

This policy is reviewed on an annual basis but might be subject to amends more frequently to comply with changes in governance and/or to address technology trends.

4. Scope

This policy applies to all users within CET including staff, pupils, trustees, governors, volunteers, Visitors and contractors.

5. Passwords

5.1 Staff

Follow these guidelines to ensure IT passwords conform to the best practice guidelines:

- **Never** use personal information, telephone numbers, names, locations or contacts within your organisation can all be guessed.
- **Never** use passwords that contain the user account name or any other personally identifiable information (date of birth, address, name of pet, for example).
- **Never** follow a theme for passwords such as the names of movies for a specific actor.
- **Never** keep any element the same. Always ensure the whole password changes, for example: An old password of 'indigo123!', shouldn't be change it to 'indigo1234!'.
- **Avoid** using incrementing numbers overtime
- **Don't** make passwords obvious

- **Always** include numbers and letters and UPPER and lower case.
- **Use** a minimum of 12 of characters. Your keyboard doesn't only contain A-Z, include spaces, !.?'@'s…they are all legal password characters on good systems.
- **Spell** words with numbers (for example, w1th numb3r5).
- **Include** written numbers, like password22seventy3, if someone overhears you mention the password, it gives you extra time to change it, as it is much harder to get right.
- **Purposely** miss-spell common words used within a password
- **Combine passphrases** common words for example D0gsUnny_wA1k?
- **Use** the three random word technique, recommended by the National Cyber Security Centre with a minimum of 12 characters

Please see guidance from NCSC regarding managing your passwords.

5.2 Pupils

- All KS1 & KS2 users will be provided with a school username and password
- Pupils will be taught the importance of password security
- The password complexity will be set with regards to the cognitive ability of the students.

Pupil logins should be monitored by the class teacher and staff members, pupils should only use electronic devices under supervision

5.3 Basic password security rules

- Never write down a password and in particular never include both username and the password on the same piece of paper.
- Never send a password via an email or social media
- Do not share your password over the phone
- Never divulge passwords to anyone else, unless clear authorisation has taken place as in the case of criminal or disciplinary investigation.
- Do not share your username or password.

Please refer to the Trust's Clear Screen and Clear Desk Policy when leaving a workstation.

5.4 Lost or forgotten password

If you lose or forget your password, you must contact your school's ICT staff or provider. Where you must identify yourself as an authorised member of staff.

A password reset for pupils will be actioned if this has been requested by their class teacher.

5.5 System administrator passwords

Due to the critical and sensitive nature of system administrator usernames and

Passwords within CET, in addition to all standard password policy provisos, the following shall be mandated:

- Any username/password combination made available to third parties shall be disabled and only enabled by the responsible ICT staff or provider for the completion of a specific task e.g. fault diagnosis and only for the agreed duration of said task
- Any username/password combination shall only be made available to designated ICT staff or providers with direct responsibility of administering said systems
- Username/password combination shall not be recorded in any paper-based file

- Any locally retained username/password combination stored electronically shall be password protected and know only to ICT staff or providers with direct responsibility for administering said systems
- A series of master username/password combinations shall be created and maintained by each school's ICT staff or provider. This master list shall be sealed and stored in a secure location and can only be accessed at the request of the headteacher or CEO in the event of a major Business Continuity failure requiring the restoration of ICT systems
- A master copy of the above point for each school and Trust, shall be sealed and stored in a secure location at the CET head office and can only be accessed by the CEO, Head of school improvement and the Trust's IT Development and Data Protection Officer in the event of a major Business Continuity failure requiring the restoration of ICT systems

Please refer to your school's Business continuity plan and Cyber response plan.

6. Security incident

All security incidents, including actual or potential unauthorised access to the Trust's IT systems, should be reported immediately to their school's ICT staff or providers or to the central 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 the event that a user suspects that their password has been compromised, they should:

- Immediately seek to change the password if they are able.
- Contact their school's ICT staff or provider as soon as possible, then the account can either be suspended by disabling it, prevent any further access, or change the password.

It shall be noted by all staff and students that they are held responsible for all activity undertaken using their username and password until they are able to prove otherwise.

In the event of a breach of this Password Policy by a user, the Trust reserves the right to:

- restrict or terminate a user's right to use the Trust ICT Infrastructure;
- disclose information to law enforcement agencies and take any legal action against a user for breach of this policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith; or
- where the user is also a member of the Trust community, the Trust may take disciplinary action.

Please refer to the Trust's Disciplinary Procedure and schools Behaviour Policies

7. Monitoring

All Trust ICT systems may be monitored in accordance with the Password Policy, so personal privacy cannot be assumed when using school hardware, software or services. The Trust can monitor the usage of its own Infrastructure and services (internet access, email, Wi-Fi etc.) as well as activity on end user compute (iPads, laptops, desktop computers, Chromebook etc.) without prior notification or authorisation from Users when justifiable concerns have been raised.

8. Multi/Two Factor Authentication (MFA/2FA)

In addition, and due to the increasing risk of cyber-attack, MFA is implemented for all staff across the Trust. This additional layer of security adds a second 'factor' of authentication in addition the user's password.

In school and Trust settings, this second layer will be provided via a one-time numeric authentication code generated randomly and provided via; text message and/or the use of an authentication app. Once a user has validated their identity via username, password and one form of MFA, validation may be required from time to time or if a device hasn't been accessed by a user for some considerable time this - negates the requirement for staff to access their mobile phone while in class.

Employees are allowed to use personal devices to complete two-factor authentication (2FA) requirements.

Staff must not share or disclose their MFA factor (including any one-time codes) with anyone else.

For 365, use the Microsoft Authenticator app, which can be downloaded from Google play or App store.

For Google Workspace, use the Google Authenticator app, which can be downloaded from Google play or App store.

Other third-party cloud hosted systems that support MFA used within the Trust, MFA will be applied where possible.

9. Links with other policies

This Password policy is link to our:

- Data protection

- Acceptable use
- Clear and clear screen
- Data breach
- Disciplinary procedure
- Behaviour policies
- Privacy notice