Password Policy

1. Purpose

This is an internal policy that defines how Chelmsford County High School for Girls (CCHS) manages authentication mechanisms for information technology systems used by its staff and subcontractors.

2. Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to the CCHS's information technology systems are expected to conform to this policy.

CCHS's IT Team are responsible for providing support to users in complying with this policy.

The IT Manager is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change or compliance frameworks such as the Cyber Essentials scheme are updated.

3. Default Credentials

CCHS always changes default credentials. Default credentials are changed as a matter of priority upon receiving a new device, factory resetting a device, or commissioning a new service. Accounts and devices are never exposed to the internet before first having their default credentials changed.

4. Strong Passwords

CCHS follows the following principles when creating a new password.

- Are never obvious (easy for an attacker to guess)
- Are never commonly used passwords
- Have never been disclosed in a breach (validated using the HaveIBeenPwned service (haveibeenpwned.com)
- Are never re-used when a password expires
- Are never re-used across different accounts
- Meets the complexity requirements:
    - Minimum of 8 characters in length
    - Contains a minimum of one lowercase character, one uppercase character and one number.
    - does not contain any part of the user's name

5. Password Disclosure

CCHS staff and students will never:

- Write down their passwords or encryption keys
- Disclose their password to others

CCHS's IT Team will never ask staff and students for their password.

6. Multi-Factor Authentication

All staff and Students at CCHS will ensure that multi-factor authentication (MFA) is enabled for all devices and services that support this technology. CCHS's preferred method of MFA is via a notification on the Microsoft authenticator app.

7. Training

All staff and students at CCHS are encouraged to remain conversant with password advice from the UK's National Cyber Security Centre.

Change Log

Version	Changes	Author	Change Date	Approval Date
0.1 – Draft 1.0 - Approved	First draft based on Secure Schools Ltd model policy.	Tony Cable	13th May 2022	22nd June 2022

Approved by	Facilities & Finance Committee
Date Approved	22nd June 2022
Date of Next Review	June 2023
Model Policy	Secure Schools Ltd