CROWN PRIVATE SCHOOL مدرسة كراون الخاصة British Curriculum المنهاج البريطاني	# PASSWORD POLICY

PROCESS NAME:	Password Policy	**CREATION DATE:**	10/09/2022
PROCESS MANAGER:	IT Administrator	**LAST REVISION:**	05/02/2025
PREPARED BY	Rajeesh Kumar – IT-Admin	**APPROVED BY**	Dr. Kishor Pillai- Principal
APPLIES TO:	All Staff All Parents All Children	**RELATED DOCUMENT(S):**	Acceptable Use policy

1. Introduction

Passwords are one of the most critical lines of defense in protecting access to Crown Private School's systems and sensitive data. Weak or compromised passwords can lead to unauthorized access, data breaches, and exploitation of school resources. This policy is designed to outline best practices for creating, securing, and managing passwords to ensure the safety and security of all CPS systems and networks.

2. Scope

This policy applies to all personnel (students, staff, contractors, and vendors) who are responsible for an account or any access method requiring a password on systems that are hosted by Crown Private School or are connected to CPS's network. This includes systems that store or process non-public information within the CPS domain.

3. Policy Overview

The goal of this policy is to:

- Ensure that passwords are strong enough to withstand common attacks.
- Promote regular password changes to reduce the risk of unauthorized access.
- Standardize password management practices across CPS.
- Require multi-factor authentication (MFA) where applicable for sensitive systems.

4. Password Creation

To ensure the strength of passwords, the following criteria must be followed when creating new passwords:

- **Length**: Passwords must be between 8 and 20 characters in length.
-
- **Complexity**: Passwords must include a combination of:

  - Uppercase letters (A-Z).
  - Lowercase letters (a-z).
  - Numbers (0-9).
  - Special characters (e.g., !, @, #, $, %, ^).
- **Avoid Dictionary Words**: Passwords should avoid using easily guessable words, including common dictionary terms, user names, or repetitive characters.
- **Uniqueness**: Passwords should not be reused across different systems or accounts.

5. Password Protection

- **Storage**: Passwords must never be stored in plain text or in easily accessible files. Use password management tools where applicable.
- **Sharing**: Passwords must never be shared with anyone, including other users, staff, or contractors. If access needs to be shared, an administrative protocol for delegating access must be followed.
- **Encryption**: All passwords must be stored in encrypted form using industry-standard cryptographic algorithms.

6. Password Expiry and Change Protocols

- **Password Expiry**: Passwords must be changed at least every 90 days.
- **Immediate Change**: Passwords must be changed immediately if there is any suspicion that they have been compromised.
- **Password History**: Users must not be allowed to reuse any of their last five passwords when resetting.

7. Multi-Factor Authentication (MFA)

For systems storing sensitive or critical information, multi-factor authentication (MFA) must be enabled. Users must authenticate their identity using two or more verification methods (e.g., password and mobile authentication).

8. User Education and Awareness

Crown Private School will provide periodic training and awareness programs to ensure all users understand the importance of password security and are familiar with best practices for creating and managing passwords.

9. Enforcement

Failure to comply with this policy may result in disciplinary action. Regular audits will be conducted to ensure compliance with password management protocols.