POLICY NAME:	**PASSWORD POLICY**				
APPROVAL AUTHORITY:	**PRINCIPAL**	**ADOPTED:**	**03.05.2021**	**REVIEWED:**	**03.10.2022**
RESPONSIBLE EXECUTIVE:	**E-SAFETY OFFICER**	**REVISED:**	**15.4.2025**	**NEXT REVIEW ON:**	**15.4.2026**
RESPONSIBLE OFFICE:	**IT DEPARTMENT**	**AVAILABLE:**	**IN THE LIBRARY, WEBSITE, NLP**		

SCOPE:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of entire school's network. As such, all staff and students/parents are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Guidelines for selecting a Password

1. Poor, unacceptable passwords have the following characteristics:
   - ✗ The password contains fewer than eight characters
   - ✗ The password is a word found in a dictionary (English or foreign)
   - ✗ The password is a common usage word such as:
     - Names of family, pets, friends, co-workers, fantasy characters, etc.
     - Computer terms and names, commands, sites, companies, hardware, software
     - Acronyms for the agency or city.
     - Birthdays and other personal information such as addresses and phone numbers
     - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
     - Any of the above spelled backwards
     - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2. Strong (acceptable) passwords have the following characteristics:
   - ✓ Contain both upper and lowercase characters (e.g., a-z, AZ)
   - ✓ Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";í<>?,./)

- ✓ Are at least eight alphanumeric characters long
- ✓ Are not a word in any language, slang, dialect, jargon, etc.
- ✓ Are not based on personal information, names of family, etc.
- ✓ Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: ?This May Be One Way To Remember? and the password could be: ?TmB1w2R!? or ?Tmb1W> r~? or some other variation.

Staff Password Protection

- Only those authorised to access specific devices, information, systems are provided with the relevantpasswords, and such provisions are reviewed regularly to ensure that access is still valid and required.
- All school networks and systems will be protected by secure passwords that are regularly changed
- Passwords for new users will be allocated by the ICT technician
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log in details and must immediately report any suspicion or evidence that there has been a breach ofsecurity
- Users need to change their passwords at regularintervals
- Passwords should be different for different accounts, to ensure that other systems are notput at risk
- Passwords must not be inserted into e-mail messages, chat or other forms of electronic communication.
- Authorized staff will be provided with a password to use the school website for uploading information on the school website

Student Password Protection

- Student will be provided with separate user id and password to access the school portal to access the teaching contents.
- User ID and password will be provided by ICT technician who will keep an up to daterecord of users.
- Students are instructed to change their password on first login.
- Password for student management system should be changed regularly after 120 daysby theuser.
- In case student forgets the password, reset option is available on the website which sends a new password as SMS to the phone number registered at school.
- Awareness training will be given to students on the importance of passwordsecurity.