HASTINGS AND PRINCE EDWARD DISTRICT SCHOOL BOARD

PROCEDURE 148	
Adopted	May 2011
Last Revised	February 2024
Review Date	February 2029

STAFF PASSWORD PROCEDURE

1. PURPOSE

Passwords are an important aspect of electronic security. They are the front line of protection for user accounts. Board owned data must be secured to protect the personal information of staff and students in accordance with the *Municipal Freedom of Information and Protection of Privacy Act.* Risk management measures must also be taken to ensure accountability, promote public trust and minimize legal liability. Passwords serve to protect these resources, however a weak password, if compromised, could put the entire network at risk. As a result, all employees of the Hastings and Prince Edward District School Board are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

The purpose of this Procedure is to set a standard for creating, protecting, and changing passwords.

2. PASSWORD CREATION

a) Passwords are used to access any number of Board systems including the network, email, web applications and voice mail. Weak passwords are easily detected and can put the entire system at risk. When creating a strong password, create one that is easy to remember and includes the following guidelines. We highly encourage the use of passphrases.

b) Passphrases are short sentences or multiple words connected by a special character to create a long, memorable, and secure password. A passphrase known only by the user is an effective way to generate a strong password. Example: I like 2 spend time @ school.

c) Password/Phrases should be at least 14 characters in length and should contain a combination of letters (a mixture of upper and lower case). For enhanced security, add numbers and at least one non-alphanumeric character.
   i. Upper case characters (A...Z)
   ii. Lower case characters (a...m)
   iii. Numbers (0…9)
   iv. Non-Alphanumeric (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

d) Passwords should not be based on a user's easily accessible personal information or that of his/her family members, pets, friends, or co-workers (e.g. username, date of

birth, address, phone number, SIN, or any other unique identifying number or symbol).

i. Passwords should not be based on single common words.
ii. Passwords should not be based on the Board/school's name or geographic location.
iii. Passwords should not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx".

The following are some examples of both strong and weak passwords:

Password	Strength	Reason
charles1	Weak	User's first name used – too easy.
22965	Weak	Same as user's personal banking PIN – poses additional risks to user.
IlikeBlue@27	Mild Strong	Three words with upper and lower-case letters, a special character and a number.
It's time for vacation	Strong	Pass Phrase upper character special character over 14 characters.
Correct~Horse~Battery~Staple	Strong	Pass Phrase upper characters special characters over 14 characters.

3. PASSWORD PROTECTION

Passwords should be treated as confidential information. No employee is to share their password with another person (including ITS staff, administrators, supervisors, other co-workers, friends and family members) under any circumstances.

a) If it is necessary to keep a record of a password, then it should be kept in a safe controlled access place if in hardcopy form, or in an encrypted file if in electronic form.

b) Passwords are not to be transmitted through email or over the Internet. However, using a password retrieval feature such as "Forgot My Password" is permitted, as is typing in a password to a secure website to access Board resources via the Internet.

c) Never use the "Remember Password" feature on any public/shared system or application.

d) Passwords used to gain access to Board systems should not be used as passwords to access personal systems, accounts, or information such as home computing devices or personal web applications.

e) If an employee knows or suspects that his/her password has been compromised, it must be reported to the ITS Helpdesk and the password changed immediately.

4. PASSWORD CHANGES

The Information and Technology Services Department staff is responsible for supporting users who wish to change their password. Passwords should be changed only when there is reason to believe a password has been compromised.

The ITS Helpdesk can assist users who request to have their password changed in instances where the password is forgotten or there is a problem with the user's password.

a) Employees can change their own password using the myHPEDSB application (https://my.hpedsb.on.ca)
b) Employees can also change their Microsoft password at www.office.com or Google password at https://myaccount.google.com
c) In the event that a password needs to be reset by someone other than the user, the user's immediate supervisor must make the request.

5. MULTIFACTOR AUTHENTICATION (MFA)

MFA is an authentication method that requires users to verify their identity using independent sources instead of just asking for a username and password.

a) Staff must sign up for MFA to access data.
b) MFA will not be applied to student accounts.
c) MFA will challenge a staff member's access to data when not connected to an HPEDSB network.

MFA factor authentication will include one of the following challenges:
a) Text message to a cell phone.
b) Voice call to a phone (land line).
c) Authentication application on your device.

Legal References:
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- *Education Act*

District Resources:
- Procedure 147: Technology Use

External Resources:
- ECNO Cyber-Awareness