COMPUTER PASSWORD POLICY

Employees and students at Patchogue-Medford School District access a variety of IT resources, including computers and other hardware devices, data storage systems, and other accounts. Passwords are a key part of Technology's strategy to make sure only authorized people can access those resources and data.

All employees and students who have access to any of those resources are responsible for choosing strong passwords and protecting their log-in information from unauthorized users. The purpose of this policy is to make sure all Patchogue-Medford School District resources and data receive adequate password protection. The policy covers all employees who are responsible for one or more accounts have access to any resource that requires a password.

Your password is more than just a key to your computer or online account. It is a gateway to all of your important information. If your password falls into the wrong hands, a cyber criminal can impersonate you online, access your bank or credit card accounts, sign your name to online service agreements or contracts, engage in financial transactions, or change your account information.

Unfortunately, many users are still not taking necessary steps to protect their accounts, such as using strong passwords. Far too often, passwords with simple combinations such as 123456, password, qwerty, or abc123 are being used. In other cases, people simply use their pet's name or their birth date -- information that can be easily found online, such as on a Facebook or genealogy page.

Password Creation

- Passwords must have at least eight characters and include upper case (capital) and lowercase letters, numbers and symbols. These requirements will be enforced with software where possible.
- Do not use words and proper names, regardless of language. Hackers use programs that try every word in a dictionary.
- Do not use personal information -- name, children's name, birthdates, etc. that someone might already know or easily obtain.
- If it appears that an unauthorized person has logged in to an account; the password must be changed immediately and the District's IT department should be notified.
- Use different passwords for each account you have.
- Make sure your work passwords are different from your personal passwords.
- Default passwords - such as those created for new employees when they start or those that protect new systems when they're initially set up they must be changed as soon as possible.

Computer Password Policy (Continued)

Protecting Your Passwords

- DO NOT write down your passwords. If you need to remember your passwords, write down a hint to a password, but never the password itself. Store the hint in a safe place away from your computer.
- Do not share your password with anyone – attackers may try to trick you via phone calls or email messages into sharing your password.
- Do not reveal your password on surveys, questionnaires or security forms.
- Decline the "Remember Password" feature in browsers.
- Always remember to logout when you will be away from a District computer.

Adopted:
April 23, 2018
Reviewed:
June 29, 2020
Revised:
March 21, 2022