Pekin Public Schools User Password Policy

Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at Pekin Public Schools District 108.

Scope

This policy shall apply to all employees, contractors, and affiliates of Pekin Public Schools District 108, and shall govern acceptable password use on all systems that connect to Pekin Public Schools District 108 network and access or store Pekin Public Schools District 108 data.

Policy

Password Creation

1. All passwords must be at least eight [8] characters in length.
2. Passwords must contain three of the following four categories:
    a. English lowercase letters (a - z)
    b. English uppercase letters (A - Z)
    c. Numbers (0 - 9)
    d. Non-alphabetic characters (!#$:%*&,.?)
3. Passwords must not contain your account name or parts of your full name that exceed two consecutive characters.
4. Passwords must be completely unique, and should not be used for any other system, application, or personal account.

Password Aging

1. User passwords must be changed a minimum of once every six to eight months. Forced password changes will take place in August when the new school year starts and again in January when classes resume after break. However, passwords can be changed at any time and more frequent password changes are encouraged but not required.
2. Old passwords can only be reused on the sixth password change; you must have used at least five unique passwords before any can repeat.

Password Protection

1. Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
2. Passwords shall not be written down or physically stored anywhere in the classroom or office.
3. When configuring password “hints,” do not hint at the format of your password (e.g., “zip + middle name”)
4. “Remember Password” feature on websites and applications should not be used.
5. User IDs and passwords must not be stored in an unencrypted format.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above. If you believe your password may have been compromised, please **immediately** report the incident to the Tech Center and change the password.

Exceptions

There may be times when Tech Center staff need to access your domain and/or G Suite account in order to troubleshoot/fix problems. We will always try to coordinate access with you, but in the event that we need access and you are not available we will reset your password to the default password and you will need to change it the next time you access your account.