Administrative Procedure 620

STRONG PASSWORDS

Background:

Aspen View Public Schools will ensure that personal or sensitive data will be appropriately protected by strong passwords and standard operating procedures in accordance with applicable legislation.

Procedures:

1. Personal, private and/or sensitive data should be saved to Aspen View's internal servers or cloud based services approved by Aspen View for storage of personal information, not hard drives or external storage devices (flashdrives, CD's, DVD's, etc.).

2. Where appropriate, laptops and other mobile computing devices should be encrypted to an industry standard as determined by the Technical Services Department.

3. Strong Passwords must be used in accordance with the following:

   Students, Grades 0 – 3

   1. No requirements for strong passwords.

   Students, Grades 4 – 7

   1. 6 Characters or more in length.

   2. 6 previous passwords will be remembered.

   3. Set at beginning of year and will not be reset during the year. All passwords and student accounts are deleted at the end of the school year (Do we need to delete student accounts?).

   4. Must wait 1 day after resetting password to reset it again.

   5. Account will be locked out for 15 minutes if 10 failed login attempts are made in a 15 minute period.

Students, Grade 8 – 12

1. 8 Characters or more in length

2. Must meet complexity requirements by having 3 of the following 4
   a. English uppercase characters (A through Z)
   b. English lowercase letters (a through z)
   c. Base 10 digits (0 through 9)
   d. Non-alphabetic characters or symbols (for example: !, @, #, $, %, ^, &,)

3. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters

4. 6 previous passwords will be remembered.

5. Set at beginning of year and will not be reset during the year. All passwords and student accounts are deleted at the end of the school year

6. Must wait 7 days after resetting password to reset it again.

7. Account will be locked out for 15 minutes if 6 failed login attempts are made in a 15 minute period.

Administrators, Teachers, Support Staff, Substitute Teachers, Partners

1. 10 Characters or more in length.

2. Must meet complexity requirements by having 3 of the following 4
   a. English uppercase characters (A through Z)
   b. English lowercase letters (a through z)
   c. Base 10 digits (0 through 9)
   d. Non-alphabetic characters or symbols (for example: !, @, #, $, %, ^, &)

3. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.

4. 6 previous passwords will be remembered.

5. Reset once per year.

6. Must wait 7 days after resetting password to reset it again.

7. Account will be locked out for 15 minutes if 6 failed login attempts are made in a 15 minute period.

Reference: Freedom of Information and Protection of Privacy Act
NIST https://en.wikipedia.org/wiki/Password_policy#Usability_considerations