PASSWORD STANDARDS

PURPOSE

The purpose of this document is to establish password standards to ensure the security and integrity of Deerfield's network and systems. Strong passwords are crucial to protecting our data and resources from unauthorized access. This document outlines the requirements for creating, managing, and maintaining passwords within our network.

SCOPE

This policy applies to all employees, students, vendors, and guests who access or manage the Academy's network and information systems.

PASSWORD REQUIREMENTS

Password Complexity

Passwords must meet the following complexity requirements:

1) Length: Minimum of 15 characters.

2) Character Set: Must include at least three of the following four character types:

   - Uppercase letters (A-Z)
   - Lowercase letters (a-z)
   - Digits (0-9)
   - Special characters (e.g., !, @, #, $, %, ^, &, *, including a space)

Password Uniqueness

Users must not reuse any of their last 5 passwords.

Avoid Common Passwords:

Passwords must not be easily guessable or commonly used. The following words are restricted and may not be used in Deerfield passwords:

- Deerfield
- Academy
- 1797
- Boyden
- password
- Albany