Password Protection Best Practices Requirement

Subject: Appropriate password protection in the school environment
Effective: September 2019

OVERVIEW, PURPOSE, SCOPE

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of *Seaside School District*'s entire network. As such, all *Seaside School District* employees (including contractors and vendors with access to *Seaside School District* systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

The purpose of this procedure is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this procedure includes all personnel who have or are responsible for an account on Windows/Synergy/Email (linked) and/or Infinite Visions.

PROCEDURE

Frequency

- **Windows/Synergy/Email (linked):** All user-level passwords must be changed every 180 days. This includes all staff with an electronic communication account. Password changes will be prompted automatically.
- **Infinite Visions:** All systems-level passwords must be changed at least every 180 days. Systems level users include the Technology Coordinator, Business Manager, Payroll and Accounts Receivable. Password changes will be prompted automatically.

Password Construction Requirements

- Be a minimum length of twelve (12) characters (pass-phrases are easier to remember, e.g. thequickbrownfox) and;
- Not be identical to the previous three (3) passwords.

Password Protection Standards

- Do not use your User ID as your password.
- Do not share your login credentials with anyone, including other school district staff.
- All passwords are to be treated as sensitive, confidential Seaside School District information.