

**The School Board of Wayland-Cohocton Central School District
(SB-WCCS) Information Technology Department (ITD)
Information Technology Policy and Procedures**

STAFF PASSWORD POLICY

Adopted by The Board of Education September 22, 2008

Username and Passwords

Security is a fundamental necessity for safeguarding information. Consistency and reliability are paramount for the SB-WCCS network to serve its users.

The Technology Coordinator shall supply each duly authorized user with an initial username and password that will permit the user to sign on to the SB-WCCS network. At first logon, users must create a password that meets the following minimum complexity requirements:

- At least 8 characters long
- Does not contain your username, real name and/or company name
- Does not contain a complete dictionary word
- Is significantly different from previous passwords
- Contains characters from **three** of the following four groups:
 - Uppercase characters (A – Z)
 - Lowercase characters (a – z)
 - Numerals (0 - 9)
 - Symbols (all keyboard characters not defined as letters or numerals)

Passwords must be changed every 90 days enforced by server policy (or as required by the individual program) by the user to maintain systems' security. All passwords are to be treated as sensitive and confidential. **Users may change their password at any time if security is compromised by notifying the ITD.**

After 10 unsuccessful computer login attempts, the user will be locked out. Contact with the ITD will be necessary to establish the cause of unsuccessful attempts. Resetting the password will then proceed after verification of user account.

To secure a user's workstation, a password protected screensaver, by server policy, will initiate after 40 minutes of inactivity, requiring users to re-enter their password.

Each authorized user will be responsible for use of the computer equipment to protect all data files and computer programs, by logging off or locking the system

before leaving their workstation. All computing equipment must be shutdown at the end of each work day, on weekends, on days off, and during all vacations.

Training will take place to demonstrate the change of passwords, suggest creation of complex passwords, how to secure passwords, and which applications password changes will affect.

Disclosure of Passwords

It is a violation for any person to disclose any assigned password to any other person, except to a member of the ITD or a technical designee for problem resolution purposes, and a school principal, the Business Manager, or the Superintendent. If user is not available for logon, the ITD will change user password, and at the next logon will require user to change their password. Thus, it is the responsibility of each employee to whom a password is assigned to maintain the confidentiality of the password. Under no circumstances shall passwords be posted or kept in a place that is accessible to unauthorized persons.

Access to passwords, user data and/or program accounts by any unauthorized personnel is prohibited. It is the responsibility of the account owner to notify the ITD whenever unauthorized account access is suspected. The account owner should then change their password.