PASSWORD STRATEGY

Password Security

ALL THE DEVICES AND THE NETWORK ARE PASSWORD PROTECTED

Ensured in G-suit Platform All passwords will meet the following criteria:

- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.

All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at WPS. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every School employee should know how to select strong passwords. Poor, weak passwords have the following characteristics: - The password contains less than eight characters

The DO's in the use of Online Technology and Electronic Communication:

- Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s).

Strong passwords have the following characteristics:

- Contain between 8 and 32 characters

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)

The DONT's in the use of Technology and Electronic Communication:

- Don’t share your Passwords.
- Don't enter a password when someone is sitting beside you as they may see it.
- Don't save your username and password on the browser
- Don't use someone else's password even if it is shared with you.
- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to a supervisor.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Do not use the "Remember Password" feature of any applications.
- Do not write passwords down and store them anywhere in public.
- Do not store passwords in a file on ANY computer

If an account or password is suspected to have been compromised, report the incident to the School IT Department immediately and change all passwords as soon as possible.

Inappropriate Activities

- Revealing or publicizing confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)

For my own personal safety

- I will keep my username and password safe and secure-I will not share it, nor will I try to use any other person’s username and password.
- I understand that I should not write down or store a password where it is possible that some may steal it.

The E-Safety Coordinator has to ensure:

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

LEGAL ASPECTS

- Never read someone else's e-mails even if you know his/her password.

Account Capabilities:

• All accounts will be accessible from both inside and outside the school network. All accounts will be password protected.

• Students will have the option of forwarding school E-mails to a personal account of their choice. It is the student's responsibility to maintain the personal account and password. It is also the student's responsibility to update the forwarding address if they change their personal account provider. Once a student forwards Email from their school account, the school is no longer responsible or liable for misuse of information, loss of confidentiality, or loss of information.

• Students must understand that the school has reserved the right to conduct monitoring of these computer systems and can do so despite the assignment of passwords to individual students for system security. Any password systems implemented by the school are designed solely to provide system security from unauthorized users, not to provide privacy to the individual system user.

• In frequency of 90 days, the students are bound to change the current password before it gets suspended.

Student Responsibilities:

- Students are entirely responsible for the confidentiality of their E-mail accounts, passwords, personal information, and for any activities that occur in the use of their accounts.
- Never use any personal information such as name, date of birth, address, etc., as your password.