BHAVANS
WISE
INDIAN ACADEMY

Policy /Password Policy

Title	:	**Password Policy**
File Name	:	**WIA/ACD-PP/016**
Date of Issue	:	**22nd Nov 2020**
Revision Date	:	**17th Dec 2020**

Introduction

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

Creating a good password computers is crucial for the safety of the children. It is, therefore, good to set some policies in place while creating passwords for the computers and all online login systems.

Policy Statement

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- All users will have clearly defined access rights to school technical systems and devices
- All school networks and systems will be protected by secure passwords that are regularly changed
- The administrator passwords for the school systems, used by the technical staff must also be available to the Senior Leadership Team.
- Passwords for new users will be allocated by the IT Administrator.
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Users will change their passwords at regular intervals.

Scope

This policy applies to all members of the school (including staff, students, volunteers, parents / guardian, visitors) who have access to and are users of school ICT systems, both in and out of the school.

Policy General

- Change your passwords periodically.
- The frequency of password change is generally based on the privilege or access level of the account. Accounts with greater privilege or access should have their passwords changed more frequently.
- The minimum required interval for password changes is once every year.
- If your password has been compromised or you suspect it's been compromised, change your password immediately.
- 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.

Strong passwords are:

- At least twelve characters, (longer is better)
- A mix of upper and lower case letters (a-z, A-Z), numbers (0-9), and symbols (~!%^)+]>}`$*)
- Are not a word in any language, slang, dialect, jargon, etc.
- Something hard to guess, but easy to remember.
- Length - We recommend a minimum of six (preferably eight) characters in a password for students. The reason for this is because the time one takes to crack a password increases exponentially with its length.
- Complexity - Passwords should contain at least one alpha, one numeric and one non-alphanumeric character (a symbol).
- Repetition - Change the password on regular intervals and make sure that it is not the same as the previously used passwords. It is recommended that a user does not keep using two passwords over and over again by alternating between them.
- Privacy - Do not share passwords with anyone, passwords are to be treated as sensitive and confidential. Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, or browsers such as Firefox or Internet Explorer etc.).

Bad passwords are:

- Predictable patterns or significant repeating of the same character

- Personal information (name, birth date, family/friend/pet's names, address, SSN, etc.)
- A password you use for other systems

How can I create a memorable password?

- One way to do this is create a password based on a song title, affirmation, or other phrase.
- Think of a phrase you can easily memorize
- Keep the first letter of each word and insert numbers where appropriate
-

<u>Password Protection Standards</u>

Password protection is a vital part of any security plan, so please observe the following standards:

Do not use the same password for school accounts as for other non-school accounts, such as personal email account, benefits, banking, and other accounts.

Do not share school passwords with anyone.

All passwords are to be treated as sensitive information.

When IT works on your computer, please arrange to be available to type in your password as needed. If that is not possible, change your password immediately before and after the work is done.

Good practices to follow:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message to ANYONE
- Don't reveal a password to anyone.
- Don't write passwords down and save them.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms to ANYONE
- Don't reveal a password to co-workers/Classmates.
- Don't use the "Remember Password" feature of applications.
- Don't store passwords in a file on ANY computer system (including a smartphone or similar devices) without encryption.
- If someone demands a password, refer that person to this document or have that person call a staff member of the information technology department.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including termination of employment/Exclusion from the school as per the **Online Safety Policy** of the school.

Revision

Revision Date	File Name	Revision
22nd Nov 2020	WIA/ACD-PP/016	New policy
17th Dec 2020	WIA/ACD-PP/016	Logo change and updated

Approvals

Principal

APPENDIX A

Online Safety Policy

https://ovq.843.myftpupload.com/wp-content/uploads/2021/02/ONLINE-SAFETY-POLICY.pdf