HIGHVIEW COLLEGE
PASSWORD MANAGEMENT POLICY
Person Responsible – IT Manager

Password Management
Highview College through IT Department, is responsible for:

- Ensuring centrally managed systems are configured to enforce password controls where available in compliance with this policy;
- Educating Users on the security, creation and appropriate use of passwords;
- Ensuring compliance with licensing restrictions of centrally-managed software and applications;
- Conducting periodic audits of areas to ensure compliance with Highview College IT and password security; and
- Periodically checking the integrity of passwords on all centrally-managed systems.

The primary management tool for governing passwords is Highview College's Identity Management System (IDM). The IDM system will automatically force the standard password minimum baseline on systems connected to the IDM and maintain currency across those systems.

Systems that are not integrated with IDM will need these same standards applied manually. Any College system incapable of meeting the standard password baseline attributes as determined by the IDM system, will need to provide its baselines as an exception to the standard.

User Responsibility
Authorised Users are responsible for ensuring that their individual passwords are created and managed in accordance with this policy. All Users should be aware of this policy, their responsibilities and legal obligations.

User passwords must not be disclosed to anyone under any circumstances. This includes sharing passwords with colleagues, friends, other students or supervisors. Maintaining password confidentiality at all times is a strict Highview College requirement.

Serious breaches of this policy by staff, will be dealt with through disciplinary procedures for 'misconduct' or 'serious misconduct' and may lead to sanctions being imposed; including termination of employment [refer to the ICT Acceptable Use Policy and Enterprise Agreement].

In the case of students, appropriate action will be taken in accordance with the year level co-ordinators.

Highview College may refer any incident involving a possible breach of Territory, Commonwealth or International law to the appropriate authority for investigation.

If a security breach occurs in which a person or organisation external to the College is involved as a potential victim of the breach, the College shall refer to the external party, the details specific to that party.

Users must actively defend access to College ICT systems from unauthorised use by others, and must:

Never disclose passwords to another person. This is considered the best defence against social engineering attacks where users are manipulated into performing actions or divulging information through deceptive practice. The most common of these being phishing emails;

- Never write passwords down or leave them in a place where they could be easily found;
- Never store passwords unless they are encrypted and protected;
- Never check the "Remember my password" boxes in client software, such as Web browsers;
- Never use the same passwords for systems managed by different organizations. Using ‘Highview College’ passwords on external systems may compromise the College’s security if the external system has weaker security controls;
- Never choose a password that is a variation of your username or surname etc;
- Choose a password that is very different from the previous one;
- Never choose a password that your friends or colleagues could easily guess;
- Use a numeral within your password string, rather than as the first or last character;
- Always be wary of accidental disclosure. When entering passwords into a computer system, users should be aware of anyone in the vicinity to ensure that what is being typed cannot be seen; and Change their password as soon as possible if they suspect that someone else knows it and report any suspected breaches to the IT Department as soon as practicable.

Current College Standard Password Baseline Attributes
Minimum Password Length: 8 characters.
Password History: 5 previous passwords.
Password Age: 120 days.
Password Complexity: Complexity enabled

Password Complexity
For security reasons, your password must contain a combination of letters, numerals and nonalphanumeric characters, in both lower and upper case. This is known as password complexity. Complex Passwords enforce the following rules and restrictions:

- It must contain at least one character each from three (3) of the following four (4) categories:
- English uppercase characters (A through Z);
- English lowercase characters (a through z);
- Numbers (0 through 9); and/or
- Non alphanumeric characters (for example, !, $, #, %).
- It cannot contain any significant part of your name. e.g. If the User’s name is Fred Nee Blogs they cannot use a password containing Fred, Nee or Blogs (case does not matter); and
- It cannot contain your username or part thereof (case does not matter).

Constructing a Complex Password
There are several techniques that can be used when selecting a password that mean it will comply with the standard password baseline attributes and still be easy to remember such as using a phrase, part of a song, a famous person or a favourite thing that you will easily remember and substitute numerals for parts of it e.g. OprahW1nfrey (substituting the letter ‘I’ for the numeral 1).

Changing Passwords
All Users will be required to change their password as a minimum, three (3) times per calendar year. Any password that you suspect to have been compromised must be changed immediately and the matter must be reported to the IT Department.

Temporary Password Generation – Password Reset
If a User forgets their password they should visit the library for students or the IT Office for staff, for a reset of their password.
The IT Department or Library Staff will issue a temporary password. When issued with a temporary password, Users must change the issued password immediately following the first logon to the system. A temporary password is for single use logon only.

Standards Exception Management
The standard password baseline attributes as defined above prescribes the minimum password controls for College ICT systems. However, it is recognized that circumstances may exist where there are valid business or technical reasons why a particular system within the scope of the standard is unable to comply with one or more of the prescribed password controls.

Policy designed by Daniel Smith - 2016