Student Password Policy

Overview:

The Department's Password Policy has been strengthened to provide improved security through the use of stronger passwords, called 'Complex 7' passwords.

A safe and secure username/password is essential and will apply to all school technical systems, including networks, devices, and email. Logging onto DET sites, will remain under control of DET ICT services, where complex 7 passwords have been in use for a number of years.

1. Purpose:

1.1 The purpose of this policy is to set out and communicate the school's rules concerning the use and security of passwords that must be observed while conducting Departmental and school business, teaching, and learning activities.

1.2 The requirements defined within this policy will assist to mitigate the risk of unauthorised access to the School's Information and Communications Technology (ICT) systems and applications, thereby safeguarding the confidentiality, integrity and availability of information essential to the needs of the School.

2. Introduction:

2.1The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy.
- Logs of access are maintained by users of the system.

2.2 A safe and secure username/password system is essential if the above is to be established and will apply to all school ICT systems, including email.

3 Responsibilities:

3.1 The management of the password security policy will be the responsibility of the ICT coordinator and the Network Manager.

3.2 All students will have responsibility for the security of their username and password. Students 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.

Date: June 2017 Ratified: July 2017 Review: June 2018

DET-CRICOS-provider code – 00861K

3.3 Student users are accountable for the actions performed when their user ID and password are used to access school or Department ICT systems and applications.

3.4 System administrator/technical staff who are responsible for setting password controls must ensure that the controls comply with this policy.

4. Policy statements:

4.1 The 'administrator' passwords for the school systems, used by the technical staff, must also be available to the Principal or other nominated member of the leadership team and kept in a secure place. Consideration should also be given to using two-factor authentication for such accounts.

4.2 Passwords should not be displayed on the screen.

4.3 Passwords must not include proper names or any other personal identification about the user that might be known by others.

4.4 All school network and systems will be protected by secure passwords that are regularly changed.

4.5 The following rules apply to the use of passwords for students:

- Passwords must be a minimum of 7 characters
- Passwords cannot be more than 32 characters
- Password must be complex; that is, contain at least 1 character from three of the four following categories:
  - Lowercase characters (a-z)
  - Upper case characters (A-Z)
  - Numeric characters (0-9)
  - Special characters and punctuation (e.g.!@#$%^&*).

5. Password policy principles

5.1 Students must take reasonable steps to protect the secrecy of their passwords, including but not limited to the following:

•Students must not share their user ID and password with a third party.

•Students must not write down their password and leave it in a place where it could be easily found.

•Students must take care when typing their passwords if they are being observed.

•Students must change their password if they suspect that someone else knows it.

5.2 The Department's ICT systems and applications that authenticate users via a user ID and password must comply with the following:

•The password controls prescribed by this policy

•The clear text password is not visible on the screen when entered by the user, except on mobile devices that briefly display each password character as it is entered.

6. Training/Awareness

6.1 Students will be made aware of the school's password policy:

- In the school newsletter
- Through the school's Password Policy
- Through the acceptable use agreement

7 Audit/Monitoring/Reporting/Review

7.1 The responsible person (Network Technician) will ensure that full records are kept of:

- User IDs and requests for password changes.
- User logons.
- Security incidents related to this policy

7.2 In the event of a serious security incident the police may request and will be allowed access to passwords used for encryption.

7.3 User lists, IDs and other security related information must be given to the highest security classification and stored in a secure manner.

7.4 These records will be reviewed by at regular interviews by the principal and/or her nominee.

7.5 The policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.