ACER online assessment and reporting system

Password Guidelines

Passwords are an important aspect of online security. All users are responsible for taking the appropriate steps to select and secure their passwords. Please refer to the guidelines below about creating strong passwords and the protection of these passwords.

General Password Creation Guidelines

All users of ACER’s online assessment and reporting system should know how to select strong passwords. A password strength indicator is built into our registration process to provide you with a clear understanding of the strength of your chosen password. Strong passwords have the following characteristics:

- Contain a combination of lower case and upper case characters
- Contain numbers and punctuation symbols
- Contain ‘special’ characters e.g. @#$%^ etc
- For staff logins, contain at least ten characters
- For student logins, contain at least eight characters

Weak passwords have the following characteristics:

- The password is a word found in a dictionary (of any language)
- The password is something that can be associated with you e.g. names of family members or pets, birthday, address, phone number etc

Try to create a password that can be easily remembered, but is difficult to guess

Password Protection

It is your responsibility to ensure that your password is secure.

- Always use different passwords to access different accounts/systems.
- Do not share your password with anyone. All passwords should be treated as confidential information.
- Passwords should never be written down or stored online without encryption.
- Always decline the use of the ‘Remember Password’ feature.
- Change your password regularly.