المدرسة الإنجليزية الخاصة

**THE ENGLISH PRIVATE SCHOOL**

**Umm Al Quwain**

**Tel : +971-7649799, Fax : +971-7649899**

**Website : www.teuaq.com email : teschool@emirates.net.ae**

# *PASSWORD POLICY & GUIDELINES*

All School Staffs are responsible for safeguarding their **Login & Password Credentials** and must comply with the password parameters and standards identified in this policy. Passwords must meet the complexity requirements outlined and must not be shared with or made available to anyone in any manner that is not consistent with this policy and procedure.

## PASSWORD REQUIREMENTS

We encourage the use of strong passwords for all System Uses.

A strong password is one that is more secure by virtue of being difficult for a machine or a human to guess. Password strength can be achieved by incorporating the following characteristics; the more characteristics you incorporate into your password, the stronger it will be.

## STRONG PASSWORD CREATION

### CHARACTERISTICS OF STRONG PASSWORDS

- At least **8 Characters**—the more characters, the better
- A mixture of both **Uppercase and Lowercase letters**
- A mixture of **Letters and Numbers**
- Inclusion of at least one **Special Character**, e.g., **! @ # ?** ]

## PASSWORD CHANGE

- Change System Level Passwords once in every 3 Months or if you know or suspect that the account has been compromised.
- Change Personal Passwords once in every 6 Months or if you know or suspect that the account has been compromised.
- Do not Re-Use the Passwords

## PASSWORD PROTECTION

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Any user suspecting that his/her password may have been compromised must report the incident to the IT Department and change the passwords.

****