LEADERS PRIVATE SCHOOL, SHARJAH

Password Policy

A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment.

- All school networks and systems will be protected by secure passwords that are regularly changed.
- Passwords for new users(including staff and students) will be allocated by the IT team.
- 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 in details and must immediately report any suspicion or evidence that there has been a breach of security.
- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- If forgotten, password can be reset by the IT team upon formal request.

All passwords will meet the following criteria:

- Contain between 8 and 32 characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- Does not contain personal information, names of family, etc.

Do Not:

- reveal a password over the phone to ANYONE.
- reveal a password in an email message.
- reveal a password to a supervisor.
- talk about a password in front of others.
- hint at the format of a password (e.g., "my family name").
- reveal a password on questionnaires or security forms.
- share a password with family members.
- reveal a password to co-workers.
- reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.
- use the "Remember Password" feature of applications .
- write passwords down and store them anywhere in your office.
- store passwords in a file on ANY computer.