مـدرسـتـنـا الثـانـويـة الإنجـليـزية، الشارقة
OUR OWN ENGLISH HIGH SCHOOL, SHARJAH
A GEMS SCHOOL

GEMS EDUCATION

PASSWORD POLICY

Implemented   **: April 2020**

Reviewed   **: May 2024**

Next Review   **: May 2025**

Compiled by: SLT &SMT/IT Engineer

Approved by: Ms. Asma Gilani, Principal & CEO

Contents

1. Policy Statement

Access to all school systems shall be granted after user authentication, in order to prevent unauthorized access and enforce user accountability**.**

2. Purpose
The purpose of this policy is to establish a standard for the selection and maintenance of strong passwords.

3. Scope
All OOS staff, students and parents

4. Requirements
- All users shall be responsible for selecting and maintaining passwords according to the requirements of this document;
- All users shall adhere to the following practices to safeguard their system/application credentials:
- Shall not use a common password across school system/application accounts and their personal accounts;
- Shall not share passwords with anyone including colleagues, administrative assistants or secretaries;
- Shall not reveal passwords in emails, chats or other forms of digital or verbal communications;
- Shall not provide hints on the password format;
- Shall not store/save passwords in text files, note books, emails or web browsers;
- Shall treat passwords as company confidential information;
- Shall decline the use of the "Remember Password" feature on web applications;
- Shall not transmit passwords over a network in clear text or publicly display them.
- All questions or support issues shall be addressed to the school IT Engineer.

CATEGORY	MINIMUM LENGTH	MINIMUM COMPLEXITY	REUSE	ACCOUNT LOCKOUT	INACTIVE SESSION
User account - Administrator	14 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 6 passwords	Duration: 30 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account – Staff (except teachers)	8 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 4 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account – Teachers	8 characters	Lower case, upper case, special character and numeric digit	Expires after 90 days No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 50 minutes of inactivity
User account - Junior Students (03 and 04)	3 characters (CVC words)	Any three characters	Does not expire No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account - Mid-level Students (05 and 06)	5 characters (dictionary words)	Any five characters	Does not expire No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account - Senior Students (07 and above)	8 characters	Any eight characters	Does not expire No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity
User account - Parents	6 characters	Lower case, upper case, special character and numeric digit	Does not expire No re-use of previous 3 passwords	Duration: 15 min After 5 consecutive failed authentication attempts	Terminate after 15 minutes of inactivity

5. Guidance on selection of strong passwords

- You can choose one or two lines from a poem, song or your favourite phrase or quotation and use the first letter of each word. For e.g. 'Thing Of Beauty Is Joy Forever' becomes "Tobijf1#".

- Replace letters with numbers or characters. For e.g. "tobijf" becomes "T0b1jf#s".

- Use short unrelated words and concatenate them together with special symbol and number.

6. Policy Compliance:

School IT Engineer shall be responsible to monitor compliance with this policy.