INDIAN SCHOOL RAS AL KHAIMAH, UAE

SCHOOL POLICIES-
PASSWORD POLICY
2022-23

DECEMBER 2018
REVIEW AUGUST 1,2020
NEXT REVIEW MARCH 2021
REVIEWED ON MAY 2022
NEXT REVIEW MARCH 2021

Introduction

The School will ensure that the school network is as safe and secure as possible and that procedures within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and effectively carry out their responsibilities.

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

Definitions

Every user should be aware of how to select and use strong passwords. Users must not use weak passwords.

General Password Construction Guidelines

Strong passwords characteristics:

- At least eight to twelve characters (longer is better).
- A mix of upper and lower case letters (a-z, A-Z), numbers (0-9), and symbols (~!%^)+]>}`$*)
- Are not a word in any language, slang, dialect, jargon, etc.
- Something hard to guess but easy to remember.

Weak passwords characteristics:

- Predictable patterns or significant repeating of the same character
- Personal information (name, birth date, family/friend/pet's names, address, reg number, etc.)
- The same password is used for other logins, systems etc.

How can I create a memorable password?

Create a password-based on a song title, affirmation, or other phrases.

1. Think of a phrase you can quickly memorise.
2. Keep the first letter of each word and insert numbers and special characters where appropriate.

   Example - Phrase: I have three furry white kitties and one puppy dog!
   Corresponding password: **Ih3fwka1pd!**

Policy Statements

- All users will have clearly defined access rights to School technical systems, devices and networks.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The administrator passwords for the school systems used by the technical staff must be only available to the Principal.
- The IT admin will allocate passwords for new users.
- All users will be responsible for the security of their username and password, must not allow

other users to access the systems using their login details, and immediately report any suspicion or evidence of a security breach. The issue needs to be reported to the IT admin or DPO of the School.

- Users need to change their passwords regularly or report any suspicious activity.

Staff login

- All staff users will be provided with a username and password by the IT admin, who will keep an up to date record of users and their usernames.
- The password should be changed at regular intervals.
- The password must not include proper names or other personal information about the user that others might know.
- Passwords shall not be displayed on the screen.
- Passwords should be different for the different accounts to ensure that other systems are not put at risk.
- Passwords should be different for systems used inside and outside of School.
- Password on Gsuite ID should be changed regularly after 90 days by the user
- Teachers will be provided with a username and password to use 'YouTube' for teaching and learning purposes.
- Teachers will be provided with a password to use the school website for uploading information on the school website.

Student login

- An awareness session will be conducted for the students about the importance of password security
- If students need to use school computers for educational purposes, systems are password protected. Students need to log in with a password provided by the teachers based on the age group of students.
- Students will be provided with a username and password for a Gsuite account and ERP solution.
- If required to connect school network, will provide students with password and login details where two levels of authentication are needed.

Training / Awareness

Users must be aware of keeping passwords secure and the risks attached to unauthorised access/data loss. This should apply to even the youngest users, even if class logins are being used.

Staff Members will be made aware of the School's password policy:

- at awareness session
- through the School's online safety policy and password policy
- through the Acceptable Use Agreement

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

- in lessons
- by conducting awareness sessions.

Audit/Monitoring/Reporting/Review

The IT admin will ensure that complete records are kept of:

- User IDs and password change requests.
- User log-on
- Security incidents related to this policy will be documented

Differentiated Password Policy Implementation