Ras Al Khaimah American Academy				
Subject: Password Policy and Guidelines			**SOP No:** RAKAA-IT-06	**Controlled Copy No:** 2
			Revision No: 2	
Written by:	**ICT Manager** Asma Odawa	**Date:** Sep 12, 2020	**Based on:** Current practice	
Checked by:	**Homeroom Teacher** Faten Matar	**Date:** May 12,2022	**Supersedes:** Sep 12, 2020	**Issued on:** May 22, 2022
Approved by:	**Principal** Sandra Zaher	**Date:** May 22, 2022	**Distributed to:** Principal (Original)	**Pages:** 8
Authorized by:	**Principal** Sandra Zaher	**Date:** May 22, 2022	**Effective as of:** May 22, 2022	
			Review date: May 22, 2022	

Contents

Policy Statement

All users (Teachers, staff members, and students) have the responsibility for the security of their passwords and usernames that they are using to access the system and must meet the password standards identified in this policy. Staff and students in RAKAA must not allow other users to use their log in details. Any suspicion that there has been a breach of security must be immediately reported to the IT department.

The school is responsible for ensuring that the infrastructure and network are as safe and secure as possible. A safe username/password is essential to safeguard the school system and to ensure that only authorized users can access the school data. Passwords are the frontline protection for the users' accounts and school information system. Therefore, users must comply and refer to this policy to safeguard their data by securing the privacy of their passwords. The password security is deep rooted and connected in the online safety policy with a reflection of effective practice.

Responsibilities

Passwords must be kept secure and confidential by both staff and students. As a result, the following principles must be followed when creating and protecting passwords:

- ✓ Passwords must be changed immediately after they are issued for the first time. Initial passwords must be securely transmitted to users, either through the IT Department or Human Resources Department. This will be sent to registered parents' mobile phone in the school's management system. IT department has Logs and audits for the same.
- ✓ Passwords must never be shared with another user for any reason or in any way that contradicts this policy.
- ✓ Staff members, including administrators, teachers, and students, must never ask others for their password. If you were asked to provide your password, or if you sign into a system and grant access to someone else using your login, you must notify the IT department.

- ✓ Passwords should never be written down and left in an easily accessible or visible location to others.
- ✓ Teachers should explain to students the importance of password security
- ✓ Users should never leave themselves logged into an application or system where someone else could use their account unknowingly.
- ✓ When issuing a password to a remote user, the password must never be sent without the use of proper protection and without confirming the user identity (If it is sent through email it needs to be encrypted).
- ✓ If a password needs to be shared for external servicing, IT department should give the authorization for the same.
- ✓ Passwords must be distinct from those used for other personal services (e.g., banking).
- ✓ Passwords must adhere to the policy's complexity requirements.
- ✓ Passwords must be changed on a regular basis, as specified in this policy, at the regularly scheduled time interval or sooner if a compromise is suspected.
- ✓ If a breach or compromise is suspected, the incident must be immediately reported to the IT department. Students are fully aware of reporting procedures when password is lost or compromised. They know to whom they need to report.

Password Requirements

The passwords issued to students by the IT department will be age appropriate so that they are easy for the student to remember and enter. Since that is not feasible in Microsoft Office 365 A3 (the formal platform used in school for learning), IT department will ensure to apply that manually while issuing the password to students or support in the reset password requests (refer to Age-Appropriate Compliant Passwords section). In the password security for the cloud systems like office 365, the school has selected complex passwords for all students and staff as the system allowed. School used parents support to communicate lower grade levels password, and the policy is aligned with UAE personal data protection law.

Passwords will still meet the following parameters, which indicate the minimum password requirements for all user accounts that use passwords:

- ✓ Minimum eight characters
- ✓ It shouldn't be based on personal information such as name, mobile number, DOB, etc..
- ✓ A mix of at least one character from each of the four-character types listed below:
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Number (0-9)
  - Special characters (such as ! @ # $ & * ( ) _ + - = { } | \ : " ; ' < > ? , . / space)

In our school management system Mograsys both staff and parents were issued strong passwords.

IT administrators of office 365 are using two factor authentication.

Password Expiration

Passwords are considered temporary and must be changed on a regular basis to prevent an attacker from using a previously discovered password. If a compromise is suspected or reported, the IT department reserves the right to reset a user's password. In the school's management system and Microsoft Office 365, the IT department has set the password expiration to six months. Users are required to follow guidelines defined below:

- ✓ At least once in every six months, passwords should be changed
- ✓ Passwords must not be reused
- ✓ When creating new passwords, at least four characters must be changed.
- ✓ New passwords must adhere to the password requirements outlined in the preceding section.

Network Active Directory Users

For network AD users the IT department has set the password expiration to ninety days in the network group policies.

- ✓ Passwords must be changed at least once every ninety days.
- ✓ Passwords must not be reused
- ✓ When creating new passwords, at least four characters must be changed.
- ✓ New passwords must adhere to the password requirements outlined in the preceding section.

Account Lockout

An account lockout policy is in effect for all systems to limit attempts to guess passwords or compromise accounts. Account lockout limits and durations are defined below.

School management system (Mograsys) accounts have the following lockout policy:

- ✓ Accounts will lockout after five invalid password attempts.
- ✓ Accounts will be locked until the IT department is contacted and the user's identity is verified (Student full name, DOB, registered mobile number, EID of parent and student) before unlocking the account.

Microsoft Office 365 user accounts have the following lockout policy:

- ✓ After 10 unsuccessful sign-in attempts (wrong password), the user will be locked out for one minute. Further incorrect sign-in attempts lock out the user for increasing durations.
- ✓ If users have trouble in signing in, they need to contact the IT department and after confirming the user identity (Student full name, DOB, registered mobile number, EID of parent and student) a new password will be issued.

Network Active Directory Users have the following lockout policy:

- ✓ After 10 unsuccessful sign-in attempts (wrong password), the user will be locked out for 30 minutes.

- ✓ If users have trouble in signing in, they need to contact the IT department.

Mobile Devices

The following minimum password/pin policy is in effect for all mobile devices such as smartphones and tablets:

- ✓ At least six complex digits
- ✓ No repeating or sequential digits like 223344
- ✓ Changed every six months.

Mobile device fingerprint readers can be used to unlock the device, but a compliant password must still be set.

Student Age-Appropriate Compliant Passwords

When issuing or resetting passwords IT department will follow the below methods listed per grade level to generate a manual password that complies with the guidelines specified in this policy.

- ✓ KG-4
  - Colors, animals, or countries will be used to form the password in addition to special characters and numbers
    - Example: lioN?371
- ✓ Grades 5-8
  - By using the first letter of each word in a phrase like the full student's name to form the password in addition to special characters and numbers
    - Example of student name: Alya Salem Ahmed Mohammed
    - Password Example: aSaM!947
- ✓ Grades 9-12
  - Combination of random letters, numbers, and special characters
    - Example: aQoye1@7

Password Reset Options

There are several options available to help users change a forgotten or expired password. The preferred and quickest method is to use the reset or forget password option available in the school used platforms. To use this method to reset your password, you must first ensure that you added a mobile number, or an alternate email and you provided answers for some security questions.

- ✓ Password Self Service
  - If you have forgotten your password, you will be required to validate your identity by providing your mobile number or the added alternate email and you may be required to provide answers for some security questions.
- ✓ Password Reset Through the IT Department for staff:
  - Through WhatsApp, Microsoft Teams, or Email
    - You need to use the school's provided email or through school's Microsoft Teams account
    - If the request for reset will be sent through WhatsApp, you need to provide the below:
      - Registered mobile number provided to the HR department during the employment process
      - Staff EID
- ✓ Password Reset Through the IT Department for Students and Parents
  - In Person
    - Reset your password through the IT department after providing a copy of parent EID (Emirates ID) and the student EID.
  - Through WhatsApp, Microsoft Teams, or Email
    - Reset your password through the IT department after providing below:
      - Student full name
      - Grade and section
      - DOB
      - Registered mobile number provided to the registration department during the admission process

- EID of parent and student

References:

- Acceptable Use Policies
- Online Safety Policy
- Staff Handbook

Agreement Form

By signing this form and turning it in to IT department you agree to the terms of the Password Policy and Guidelines.

All fields are required.

Name: _____

Signature: _____

Date: _____