المدرسة الهندية النموذجية الجديدة

NEW INDIAN MODEL SCHOOL

User Password Policy

Overview

This policy is intended to establish guidelines for effectively creating, maintaining, and protecting passwords at New Indian Model School, Sharjah. The school will be responsible for ensuring that the school data and network is as safe and secure as is reasonably possible and that:

- users can only access systems and data to which they have right of access
- users should agree to an acceptable use policy
- users should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies)
- users must not store their passwords in plain view and staff must not write down passwords.
- A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and Virtual Learning Environment (VLE)

Scope

This policy shall apply to all academic and non-academic staff, students, parents and affiliates of New Indian Model School, Sharjah, and shall govern acceptable password use on:

- all systems that connect to NIMS network
- access to e-learning platform (**Educore**)
- access to administration software and MIS
- access to google apps (**G-Suite for Education**)
- access or store sensitive data.

Password Creation

- All user and admin passwords must be at least 8 characters in length.
- Longer passwords and passphrases are strongly encouraged.
- Where possible, password dictionaries should be utilized to prevent the use of common and easily cracked passwords.
- Passwords must be completely unique, and not used for any other system, application, or personal account.
- Default installation passwords must be changed immediately after installation is complete.

Password Aging

User passwords must be changed every 3 months. Previously used passwords may not be reused. System-level passwords must be changed on a quarterly basis. Appropriate policies are enabled in Educore, ERP system and G-Suite for Education to enforce the users to reset the password every 90 days. Also, users are forced to use complex passwords.

Password Protection

- Passwords must not be shared with anyone (including coworkers and supervisors), and must not be revealed or sent electronically.
- Passwords shall not be written down or physically stored anywhere in the office.
- When configuring password "hints," do not hint at the format of your password (e.g., "zip + middle name")
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login.
- "Remember Password" feature on websites and applications should not be used.
- All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Access to Sensitive Data

- Critical accounts having access to sensitive data should have two factor authentication enabled
- This includes accounts of
    - Administration staff who have access to MIS, payroll
    - Academic staff having access to critical student information (Principal, Head of Section)

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above. If you believe your password may have been compromised, please immediately report the incident to Mr Noufal (it@nimsshj.ae) and change the password.

Acknowledgement

I have read and agree the user Password Policy and will abide to the stipulated rules and regulations.

Name of the Student**: ……**Signature: **…….**

Name of the Parent**: ……** Signature**: ……**