Members of the committee

- CEO – ACADEMIC DIVISION
- DEAN ACADEMICS
- PRINCIPAL
- ADMIN OFFICER
- SOFTWARE ANALYST- CORPORATE
- SCHOOL IT ADMINISTRATOR
- INFORMATICS HOD
- HR COORDINATOR
- SCHOOL COUNSELOR
- TEACHER REPRESENTATIVES

APPROVED BY

PRINCIPAL

Introduction

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

Effective password management will protect International Indian School's data and reduce the risk of unauthorized applications access. The policy is to establish a secure information technology environment by enforcing the use of strong passwords. Strong and complex password are the front line of protection for user's accounts. A poorly chosen password may result in the compromise of International Indian School's entire network. The purpose of this policy is to provide standards for defining domain passwords to access International Indian School IT resources such as email, academic and administrative applications, computing labs and School-owned computer systems for protecting International Indian School data and reducing the risk of unauthorized access by enforcing the use of strong passwords.

Scope

This policy shall apply to all employees, students, and parents of International Indian School School, and shall govern acceptable password use on all systems that connect to International Indian School School network or access or store International Indian School School's data.

Policy

- These statements apply to all stakeholders (Staff, Students, Parents, Vendors) of International Indian School.
- All school networks and systems will be protected by secure passwords.
- All users are clearly defined with the access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT Administrator and will be reviewed, at least annually, by the online safety group.
- All stakeholders have responsibility in securely keeping the login credentials. Ensure that other users are not accessing the systems using other user's login credentials. Any breach of security or suspicious incidents must be immediately reported with evidence.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by IT Administrator who will keep an up to date record of users and their usernames

Password

- Passwords should be long and must be over 8 characters in length.. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password must contain uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts. This will ensure that other systems are not put at risk even if anyone account is compromised.
- Passwords must not contain any personal information about the user that might be known by others
- Passwords must be changed on the first login to the system itself.
- Passwords must not kept in writing or electronically which can be accessible by others.

- Records of learner usernames and passwords for younger students/pupils are securely kept which is accessible only by the IT administrator.
- Password complexity for younger students is less (5-character maximum) and special characters are not included.
- Password requirements for older students are more complex (8 characters minimum) including special characters.
- Users are required to change their password if it is compromised. The school will reset passwords at the start of each academic year to avoid large numbers of forgotten password reset requests where there is no user-controlled reset process.
- Student will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Password enforcing will be applied to all users and systems in regular intervals (3 months) and whenever a compromise threat is detected by the IT administrator.
- The administrator have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is given using two factor authentication for such accounts.
- An administrator account password for the school systems is kept in a secure school safe. This account and password is only used to recover or revoke access. Other administrator accounts does not have the ability to delete this account.
- Any digitally stored administrator passwords is hashed using a suitable algorithm for storing passwords
- There is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Wherever user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users is allocated by

administrator. This password should be temporary and the user should be forced to change their password on first login.

- Where automatically generated passwords are not possible, administrator will provide the user with their initial password. There is a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password is temporary and the user will be forced to change their password on the first login.
- Requests for password changes is authenticated by administrator to ensure that the new password can only be passed to the genuine user
- Suitable arrangements are provided to visitors with for appropriate access to systems which expires after use. The technical team will provide pre-created user/password combinations that will be allocated to visitors, recorded in a log, and deleted from the system after use.
- All the user accounts will be "locked out" following six successive incorrect log-on attempts.
- Passwords will not be displayed on screen, and will be securely hashed when stored.

Training/awareness

It is essential that users are made aware of the need for keeping passwords secure, and the risks attached to unauthorized access/data loss. This apply even to the youngest of users. All stakeholders are taught how passwords are compromised, so they understand why things should be done a certain way

Members of staff will be made aware of the school's password policy

- During induction
- school 's online safety policy and password security policy
- acceptable use agreement

Students/pupils will be made aware of the school's password policy

- in lessons
- through the Acceptable Use Agreement
- Through activities

Audit/monitoring/reporting/review

- The IT Administrator will ensure that full records are kept of:
- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

Unacceptable Use

- Any breach of password policy will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate as per the reporting mechanism.
- Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take necessary action.

Enforcement

It is the responsibility of the end user to ensure enforcement with the policies above.

This policy is linked with all the other policies of the School.