PASSWORD POLICY
AY 2024-25

HABITAT SCHOOL
AL JURF, AJMAN

Creation Date: 20/05/2014

Last Amendment Date: March2024

Next Review Date: April 2025

PASSWORD POLICY

Introduction:

Effective password management will protect Habitat School's data and reduce the risk of unauthorized application 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 Habitat's entire network. The purpose of this policy is to provide standards for defining domain passwords to access Habitat IT resources such as email, academic and administrative applications, computing labs and School-owned computer systems for protecting Habitat 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 Habitat School, and shall govern acceptable password use on all systems that connect to Habitat School network or access or store Habitat School's data.

Policy

- These statements apply to all stakeholders (Staff, Students, Parents,Vendors) of Habitat School.
- All school networks and systems will be protected by secure passwords.
- All users are clearly defined with 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 a responsibility for 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 the IT Administrator who will keep an up-to-date record of users and their usernames

Password Creation

- 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, numbers, 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's account is compromised.

- Passwords must not contain any personal information about the user that might be known by others.
- 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.
- The administrator has an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration is given to 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 are only used to recover or revoke access. Other administrator accounts cannot delete this account.

Password Aging

- User passwords and system-level passwords must be changed every [6] months. Previously used passwords may not be reused.

Password Protection

- Default installation passwords must be changed immediately after installation is complete.
- Passwords must not be shared with anyone, and must not be revealed or sent electronically.
- Passwords must not kept in writing or electronically which can be accessible by others.
- User IDs and passwords must not be stored in an unencrypted format.
- User IDs and passwords must not be scripted to enable automatic login.
- The “Remember Password” feature on websites and applications should not be used.
- All mobile devices that connect to the school network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.
- Records of learner usernames and passwords for younger students are securely kept which is accessible only by the IT administrator.
- Students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.
- Any digitally stored administrator passwords are 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 knows the password.
- Wherever user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users are allocated by the administrator. This password should be temporary and the user should be forced to change their password on the first login.
- Where automatically generated passwords are not possible, the 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 are authenticated by the administrator to ensure that the new password can only be passed to the genuine user.
- Suitable arrangements are provided to visitors for appropriate access to systems that 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's imperative to educate users about the significance of maintaining secure passwords and the potential dangers associated with unauthorized access and data loss. This applies even to the youngest users, emphasizing the importance of responsible password management. By ensuring that all stakeholders understand how passwords can be compromised, we empower them to make informed decisions and adopt secure practices to safeguard sensitive information effectively.

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

- During induction
- Through the school's online safety policy and password security policy
- Acceptable use agreement

Students 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 maintain comprehensive records encompassing

- User Ids and requests for password changes
- User logins
- Any security incidents pertinent 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.