DELHI PRIVATE SCHOOL, AJMAN

PB No: 21900, Al Tallah 2, Ajman, U.A.E, Phone: 06-747 1111,
Email: info@dpsajman.com, website: www.dpsajman.com

Password Security Policy

Introduction

Securing sensitive data is becoming more and more difficult with users having access to so many devices,Wi-Fi and internet connectivity. Single Sign on and shared accounts means a security leak on one system could allow unauthorized access to others. Teachers and pupils have access to data, documents and systems from home, the school network via Wi-Fi from the school grounds and with cloud email and storage a lost password could give malicious users easy access to a host of systems. A safe and secure username / password system is essential and will apply to all school IT systems, including email, network, systems and VLE.

The scope of this policy includes all personnel who have or are responsible for an account or any form of access that supports or requires a password on any system that resides at Delhi Private School.

Password Protection Standards

Passwords are omnipresent in our personal and professional environments. All users provided with their own user accounts will have responsibility for the security of their usernameand password, they must not allow other users to access the systems using their log on details and must immediately change their password and report any suspicion or evidence that there has been a breach ofsecurity. VLE used for remote learning should be monitored by the teacher and students should only use under supervision.

- All users of IT services should always use different passwords for different accounts. It is advisable to have separate password for school accounts from your personal accounts.
- Do not share school account passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.

- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT or Online Safety Leader.
- Always decline the use of the "Remember Password" feature of browser applications.
- If an account or password compromise is suspected, report the incident to the IT Department of Online Safety Leader.
- New user accounts, and replacement passwords for existing users will be allocated by the IT in-charge.
- Staff and pupil accounts must be disabled on leaving the school and user data deleted after 6 months.
- School office staff should ensure that the IT helpdesk is aware of the leavers as soon as possible.
- All users must change their passwords in every 90 days to ensure systems remain secure. However, the length between changes needs to take into account, the type of user and the risk to the school if unauthorized access was gained. Similarly, the complexity of password needs to reflect the user.
- All users of school IT services should be aware of how to select strong passwords. Strong passwords have at least four of the following characteristics:
    - Lower case letters
    - Upper case letters
    - Numbers
    - Punctuation
    - “Special Characters” (e.g. @#$% etc)

    Weak passwords have the following characteristics:
    - The password contains less than eight characters
    - The password is a word found in a dictionary
    - The password is a common usage word or sequences like 1234 or abcd, etc.

Password Protection Standards

All users will register their security information while logging into their account for the first time. Elementary and Middle School students will not use any authentication method other than password. Their unique credentials will be issued to the Parents through email. Students will be asked to change their password while logging into their account for the first time. Also, students will be able to change their password as and when required by themselves. If students forget their password then their Class teacher will assist the student by resetting password through IT department.

High School students will be registered for Self-Password Reset service and is require to provide their personal email id as an additional form of authentication information. It provides additional security by requiring a second form of authentication, code form their personal email address.

Passwords are omnipresent in our personal and professional environments and without certain standards, the users will have high security risks.

- All users of IT services should always use different passwords for different accounts. It is advisable to have separate password for school accounts from your personal accounts.
- Do not share school account passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
- Passwords should never be written down or stored on-line without encryption.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to this document and direct them to the IT or Online Safety Leader.
- Always decline the use of the "Remember Password" feature of browser applications.
- If an account or password compromise is suspected, report the incident to the IT Department of Online Safety Leader.

Password Control

Characters allowed	A – Z a - z 0 – 9 @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > blank space
Characters not allowed	Unicode characters.
Password restrictions	A minimum of 8 characters and a maximum of 256 characters. Requires three out of four of the following: Lowercase characters. Uppercase characters. Numbers (0-9). Symbols (see the previous password restrictions).
Password expiry duration (Maximum password age)	Default value: 90 days.

Password expiry notification (When users are notified of password expiration)	Default value: 14 days (before password expires).
Password change history	The last password can't be used again when the user changes a password.
Password reset history	The last password can be used again when the user resets a forgotten password.

Passport Reset

Credentials are specific to user's identity. Every user, including IT in-charge, teachers, staff, and students has credentials. IT department and all staff are registered for Self-Password Reset service and is require to provide additional form of authentication information. It provides additional security by requiring a second form of authentication, such as:

- A code from an SMS text message
- Providing a code from or biometric information in the Microsoft Authenticator App

Policy Statements

The following rules apply to the use of passwords:

- The account should be "locked out" following six successive incorrect log-in attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten or need to change their passwords, shall be enforced to change immediately upon the next account log in

Audit / Monitoring / Reporting / Review

The IT in-charge will ensure that full records are kept of:

- User Ids and enabled accounts
- Security incidents related to this policy

In the event of a serious security incident, the law enforcement may request and will be allowed access to passwords used for encryption.

User lists, IDs and other security related information is given the highest security classification and stored in a secure manner.

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

- at induction/orientation
- through the policies of the school, including, Online Safety Policy, Password Security Policy and Acceptable Use Policy

- through lessons related to cyber safety and digital citizenship.

These records will be reviewed by Online Safety Leader / Online Safety Group / Online Safety Governor annually in response to changes in guidance and security incidents.

Updated on 12th April, 2022