DENVER PUBLIC SCHOOLS | Department of Technology Services

Last updated: October 17, 2018

Guidelines for Passwords/Passphrases

Purpose

To safeguard all DPS electronic information, DPS has established these guidelines in support of the Board Policy - EGAEA-R1, "Regulation of Use of Electronic Mail and Internet Systems". These guidelines set out specific responsibilities, conditions and practices to minimize risk and maximize the protection of data.

To ensure passwords are strong and to safeguard information against hackers, DPS has chosen to follow the recommended guidelines for passwords from the National Institute of Standards and Technology (NIST). The NIST recommendation is to set the minimum password length to 12 characters. DPS recommends users create a password that is a phrase or a sentence. Another very important step to protecting your online identity is to never, ever repeat passwords across your various online accounts.

Password Syntax Compliance Rules

User Group	Length	History kept	Password reset
Students less than 6th grade	12 Character minimum	Last Five (5)	Breach detected or requested by student
Students 6th grade and above	12 Character minimum	Last Five (5)	Breach detected or requested by student
Parents	12 Character minimum	Last Five (5)	When breach detected and Self Service
Staff (Employee and Non-Employee)	12 Character minimum	Last Five (5)	When breach detected and Self Service

Parents/Employees/Non Employees

All parents, employees and contractors with system access are responsible to reset their own password. One tool provided by the district follows the industry standard 2-Factor Authorization, sending an authorization code to their personal email. Alternative methods for resetting a password are provided for users with DPS owned machines.

In the event a user needs additional support to reset their password, proper verification will be required in order to verify authenticity of the reset.

Users will not be required to change their password on a periodic basis. However, in the event a breach has been detected or a known sharing situation has occurred, the user will be required to reset their password.

Students
At account creation, a default password will be provided to the student.

In the event a student needs support to reset their password, proper verification will be required in order to verify authenticity of the reset. Passphrases will be provided to the student.

Students will not be required to change their password on a periodic basis. However, in the event a breach has been detected or a known sharing situation has occurred, the student will be required to reset their password.

Student Password Managers
Password Managers will have privileges to reset the passwords for the students in their assigned building(s) only.

Access will be granted based on approval by a principal or designee (normal access security request process).

DoTS InfoSec
There will be an annual review of the users by the InfoSec to ensure accuracy of the Password Reset Administrators security.

Password requirements and passphrases will be managed by InfoSec and communicated as necessary to user groups. In the event of an identified breach, the user's password will be reset.