Catalina Foothills School District

Password Guidelines

Purpose:

The Catalina Foothills School District (CFSD)'s Password Guidelines document is intended to provide general guidance in constructing a secure and appropriate password. Additionally, CFSD's Password Guidelines aim to define the password requirements for common systems.

Scope:

To secure CFSD resources and personal data, all staff and students are encouraged to follow CFSD's Password Guidelines. Third Party Vendors, Contractors, and Subcontractors are expected to use secure and appropriate passwords. Some CFSD passwords have guidelines set by vendors with little configuration permitted by CFSD's Educational Technology Department. Users should work with the specifications set by the vendor.

When feasible, CFSD will specify minimum password requirements for ease of user accessibility. The National Institute of Standards in Technology (NIST) has released password procedures that CFSD uses as guidance on setting passwords that are tough to crack yet easy to use. For more information on NIST please visit https://www.nist.gov/.

Guidelines:

Many CFSD systems have specific password requirements. For all other systems, the following best practices should be observed:

- A password should be at least eight (8) characters in length.
- A password should contain at least three (3) of the following character types:
    - Uppercase letters
    - Lowercase letters

    - Numbers
    - Special characters, such as !@#$%^&*()-=?;:
- A space character should not be used.
- A password should not be similar to the user's five most recent passwords.
- A password should not contain the user name.
- A password should not be a dictionary word.

Every user should make every effort to protect their password. Compromise of a user password may enable access to CFSD systems, but could also jeopardize the user's personal and confidential information. All users should take the following measures to protect their passwords:

- Do not use the same password for CFSD accounts and personal accounts.
- Do not share a password over the phone.
- Do not share a password in an email.
- Do not give hints regarding the format of your password.
- Do not share a password in any paper or online form.
- Do not write passwords down or try to hide them (such as under the keyboard).
- Do not store passwords in any unencrypted file.
- Do not utilize the "Save Password" feature of applications or web browsers.