GCSD Password Policy

Overview

The purpose of this Galena City School District (GCSD) password policy document is to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change. Passwords are the most frequently utilized form of authentication for accessing District resources. Due to common passwords use, the proliferation of Artificial Intelligent (AI) programs, and the activity of malicious bots and phishing attacks, passwords are often the weakest link in securing data. A poorly chosen password may result in unauthorized access and/or exploitation of GCSD resources, including the confidential data of students, alumni, applicants, faculty, and staff. All users, including contractors and vendors, with access to GCSD systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Notice: It is required that staff login passwords be changed at least every 6 months. Select staff with access to sensitive data may be required to reset passwords more frequently.

This policy applies to all users of computing resources owned or managed by GCSD. Computing resources include all licensed or managed hardware and software (including telephone and internet equipment) owned by the District, and use of the network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Specific users bound by this policy include:

- GCSD students, alumni
- Faculty, including full-time, part-time employees.
- Members of 3rd-party organizations given access to District systems, such as vendors, contractors, or consultants
- Guests

Password Policy

All passwords for GCSD systems and applications (e.g., email, web, digital devices, etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity, and frequency of changes. Use of multi-factor authentication is strongly encouraged when available (such as GCSD Microsoft 365 E-mail, OneDrive, etc.) and may be required by all staff when

accessing high-risk systems, such as those containing restricted or confidential information or other systems that may require this to register machine secure login verification information.

Password Creation

All passwords must meet the following minimum standards, except where technically infeasible. Longer passwords that utilize passphrases are inherently more secure because it takes longer to brute force. Please make your password longer and add the required complexity requirements.

Number of characters	Requirement
12 minimum	Requires at least 1 of each: upper- and lower-case letter, number, and special character. Note: Password cannot be any of the last 5 passwords used and cannot be changed sooner than 10 days apart.

Here are a couple of suggestions for making long passwords:

- Transform a memorable phrase such as "What would an ideal Chicken look like? A lot like this!" into a password such as this: "WwaiCoL?AlLt!"
  - **Please do not use this suggestion as your password!**
- To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers, DOB, account numbers, should not be used as a user ID or a password.
- Your staff password should be a password that you have not used someplace else.

Password Management

- All passwords are to be treated as confidential information as defined in GCSD's Board Policy and should therefore never be written down or stored electronically unless properly encrypted.
- Only use the "Remember Password" feature of a software application, if you are assured that the feature stores your credentials in a secure, encrypted fashion on an encrypted District device. Modern web browsers offer password managers that encrypt your password with your sign-in credentials. For this reason, you are strongly advised to never store your

password if you are on a public kiosk, unencrypted smartphone, unencrypted laptop, desktop, tablet or public lab computer.

- Unencrypted passwords should never be inserted into email messages or other forms of electronic communication. Communicate passwords to people verbally over the phone or in person.
- Do not use your GCSD password for any other systems external to District (e.g., 3rd-party vendor sites, personal web accounts, etc.). Should those systems become compromised, someone could use those credentials to access your District account.
- **It is requirement that staff passwords be changed at least every 6 months**, unless a shorter change interval is mandated (such as computers subject to the PCI Data Security Standard (those that take credit cards), which require passwords to be changed every 90 days).
- Individual passwords must not be shared with anyone, including administrative staff, IT personnel or family members. Please see exception for password-protected District documents (below).
- Password-protected documents (i.e. locked for editing, printing or downloading) must have appropriate access documentation for administration and must be registered with the IT Department to ensure access during any staff transitioning.
- Any user suspecting that their password may have been compromised must immediately change the password and report the incident to the IT Department.
- Bypassing password security to access a GCSD system is strictly forbidden.
- GCSD may perform automated security tests on a periodic or random basis. If a password is guessed or cracked during one of these scans, the password owner will be notified and be required to change it immediately.
- Password guessing or repetitive testing by unauthorized users is forbidden.

Software Administration

Currently installed selected software/hardware/services have been provided based on security and compatibility with the supported processes/network/vendors. Each has been thoroughly researched, vetted, implemented and streamlined for administration.

The ability to add unregistered applications to GCSD-assigned devices is restricted. Special requests may be considered on a case-by-case basis and must be submitted to webhelpdesk@ideafamilies.org or helpdesk@galenanet.com.

Any and all software/hardware/services will be installed by the IT Department.

Example of prohibited content: personal software, redundant software, e.g., video/audio streaming services, tax preparation, copyrighted material sharing, etc.

Violations

Anyone found in violation of this policy shall be subject to appropriate disciplinary action. Individuals are also subject to GCSD Board Policy, Federal, and Alaska State law governing all digital interactions. This document is subject to change as required. Update notices will be sent via mass communication to staff and links to the current file will be provided on the District website.

Changing your Password

To change your password, use CTRL + ALT + DEL > select change password from your District laptop, or desktop. Additionally, the IT department may issue you a temporary login that will require you to update your password after use.