Purpose
The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and verification of identity.

Scope
The scope of this policy includes all Ogden Preparatory Academy (School) employees, contractors, temporary workers, volunteers and others who have access to Ogden Preparatory Academy information resources with user ID and password authentication. All user IDs created on any Ogden Preparatory Academy computing system or device must have an associated password that meets the standards of this policy. It is the responsibility of the Ogden Preparatory Academy employee, contractor, temporary worker, volunteer, or other to adhere to this policy.

Background
Common, default or shared passwords are ineffective and aid hackers and others in their illicit attempts to access systems and confidential data within Ogden Preparatory Academy. Protecting the Ogden Preparatory Academy computers, systems, and data from unauthorized access is of preeminent importance. Strong passwords play a critical role in preventing unauthorized access.

Exceptions
A detailed case for non-compliance must be established and the request for exemption approved in advance through a risk acceptance process where the Administrative Staff or authorized designee is notified and approval for the exception is granted.

Definitions
User IDs and passwords protect the integrity of information, provide authentication, control access, and establish user audit capabilities within the Ogden Preparatory Academy computing environment and information resources. The combination of a user ID and password provide individual user validation that the person has authorized access to the system or device.

A Supervisor level password would include administrative privileges to both applications and systems. Examples include system access to an operating system on a server by a system

administrator or the ability to manage an application by an application administrator or power user.

User level passwords provide basic access to applications and systems. For example, access to email or a school application such as the school SIS system require user level passwords.

Policy

Frequency of Change
All employee level passwords must enforce two step authentication in addition to a password to ensure the identity of the user. All employee level users have access to update passwords at any time. Student level passwords must be changed by an authorized designee only. After six consecutive unsuccessful password attempts a user account will be disabled until the password is reset by the user/authorized designee.
Note: Employee level users can reset passwords using the "Forgot Password" link from the authentication screen.

General Password Construction Guidelines
All employee and student level passwords must conform to the guidelines as described in this section for selecting a strong password.

Strong passwords have the following characteristics:

- A password should be at least eight characters in length.
- Passwords should not include any portion of your name, address, date of birth, Social Security Number, username, nickname, family name, pet name, sports team name or word that appears in a dictionary or any such word spelled backward.
- Passwords must have a combination of letter, numeric digits and capital letter.
- Passwords must include at least one character from three of the following attributes:
    - Uppercase characters (A-Z)
    - Lowercase characters (a-z)
    - Numeric Characters (0-9)

When changing a password it is not acceptable to simply add a number to the end of a previously used password. Example: password88, password89, etc.

Password Creation Suggestions

Users should create passwords that can be easily remembered but not easily guessed. One way to do this is to create a password based on a song title, affirmation, or other phrase.

Examples of ways to create passwords:

"At work I am on my best behavior." The password could be: "@wIaombb"

"Money is a good asset to have." The password could be: "$isaga2h"

"The number 7 is a lucky number." The password could be: "T#7isal#"

Password Protection Standards

- Passwords must never be sent digitally in clear text including via e-mail, chat, instant messaging, or any other form of digital information transfer.
- Passwords should never be stored in unsecured places, such as written down on a sticky note or saved unprotected on-line.
- Passwords used for the Ogden Preparatory Academy computing environment and information resources should be different than those used for personal accounts (e.g., a personal ISP account or personal email accounts, benefits, banking etc.).
- User IDs and passwords should never be shared with anyone, including administrative assistants, co-workers, family members, a local network administrator, desktop technician, or supervisor.
- All passwords are to be treated as sensitive, confidential Ogden Preparatory Academy information.

If a Password or User ID is Compromised

Any time a user ID or password is suspected of being compromised, the password must be changed immediately, or a request made that the account be disabled.

Enforcement

Violation of this policy may be the basis for discipline including, but not limited to, legal penalties as prescribed by Ogden Preparatory Academy, federal statute or regulation, and termination.

Document History

Approved: 12/14/2017

Legal References