Living Sky School Division No. 202

Administrative Procedure (AP) Manual

Procedure Name: Passwords for Electronic Devices			
Procedure Type:	School Operations	**Implementation Date:**	APR. 13, 2016
Procedure Number:	4.47	**Last Approval Date:**	MAY 11, 2022
AP Owner:	IT Specialist	**Last Reviewed:**	DEC. 2, 2024
Legal Reference(s):	CIS Controls Password Guide		

Background

It is the responsibility of all users of information communications systems and services, including but not limited to all students, teachers, staff, Board of Education members and contracted parties, to comply with this procedure in conjunction with the 4.37 *Responsible Use of Technology* procedure.

This document defines requirements for:

- protecting the confidentiality and reducing the risk of inappropriate or malicious access to information regarding students, staff, parents, or system data in the digital environment;
- preventing unauthorized use of systems, resources, and other assets;
- mitigating the risk of disruption to systems and services by malicious entities or autonomous threats; and
- adhering to compliance standards set by the Office of the Provincial Auditor and other professional and regulatory bodies.

Scope

This procedure will be enforced through Active Directory or mobile device management services that provide authentication to Division systems, services, and devices. Any systems or services in use for Division purposes are subject to this procedure.

Procedures

1. Administrative, Instructional and Support Staff Passwords and PINs

a. Passwords

i. Must be at least twelve (12) characters in length.

ii. Must be changed upon request.

iii. Must contain at least one character from three of the following groups;

- Uppercase letters,
- Lowercase letters,
- Numbers, and Symbols.

iv. Cannot contain more than three sequential characters.

v. Cannot contain the users' first or last name

vi. Must not be any of the users' previous three passwords.

b. Mobile or Tablet PINs.

i. Must be at least four characters.

c. User accounts and passwords may not be shared without explicit authorization of the IT specialist or designate.

d. Personal devices accessing Division systems and services in ways that do not require authentication may be subject to this policy.

2. Elementary School Students

a. Passwords;

i. Must be at least eight (8) characters in length,
ii. Must contain at least one letter and either a number or a symbol,
iii. Cannot be words related to their respective schools,
iv. Cannot contain more than three sequential characters, and
v. Must not be any of the users' previous three passwords.

b. Passwords may be shared with homeroom teachers or educational assistants for classroom management purposes.

c. Passwords may be reset by school staff using the Student Password manager for their school or en masse via a help desk request.

c. PINs are not required for registered and managed tablets or mobile devices.

3. High School Students

a. Passwords:

i. Must be at least ten (10) characters in length,
ii. Must contain at least one character from three of the following groups;
- Uppercase letters,
- Lowercase letters,
- Numbers, and
- Symbols.

iii. Cannot contain more than three sequential characters.
iv. Cannot contain the users' first or last name
iv. Must not be any of the users' previous three passwords.

b. Students with IIPs may share passwords with homeroom teachers or educational assistance for classroom management purposes.

c. Passwords may be reset by school staff using the Student Password Manager for their school or en masse via a help desk request.

d. PINs are not required for registered and managed tablets or mobile devices.

4. Parents

a. Passwords;

i. Must be at least eight (8) characters in length, and
ii. Must not be any of the users' previous three passwords.

5. IT Administrative and Service Accounts

a. Passwords;

i. Must be at least sixteen (16) characters in length,
ii. Must be changed every 365 days,
iii. Must contain at least one character from three of the following groups;
- Uppercase letters,
- Lowercase letters,
- Numbers, and
- Symbols.

iv. Will be generated randomly,
v. Cannot contain more than four sequential characters of your username or full name, and
vi. Must not be any of the users' previous three passwords.

b. Devices, services, or accounts undergoing troubleshooting actions may be exempted from the password policy for the duration of the work.

6. Guests and Outside Contractors

a. Passwords;
i. Must be at least eight (8) characters in length,
ii. Must expire after a defined number of days or be disabled when not in use,
- If duration is not defined, the default will be eight hours.

iii. Must contain at least one character from three of the following groups;
- Uppercase letters,
- Lowercase letters,
- Numbers, and
- Symbols.

iv. Cannot contain more than three sequential characters .

b. Public access to the wi-fi is permitted.

7. Generic Use Accounts

a. The use of generic accounts for authentication purposes is otherwise prohibited.

8. Non-compliance and Appeals

a. Discovery of a user sharing their password will result in the resetting of that user's password.

b. Users of devices contravening this policy may have access to systems and services restricted through technical enforcement until corrective action is taken to rectify the discrepancy. Technical enforcement can include;
- Quarantine or removal of devices,
- Disabling user accounts, and/or
- Restricting access to software, apps and/or websites.

c. Efforts to circumvent the enforcement of this policy can result in sanctions, disciplinary actions, professional review, or criminal prosecution.

d. In the event of an appeal of the application of a technical lock, a three-party committee consisting of a senior administrator (Service Lead), a curriculum or learning representative (consultant), and a member of the Information Technology team (Technology Manager) will convene and issue a binding resolution.

Related

Procedure 4.37 - Responsible Use of Technology