



STAFF ACCOUNT MANAGEMENT

Responsibility:	<i>Superintendent, Student Achievement & Well-Being Senior Manager, Information Technology Services</i>
Legal References:	
Related References:	<i>AP 4010 - Staff Devices Disposition and Account Management – Staff Change of Location or Termination of Employment with the Board; AP 4070 - Responsible Use Procedure for Information, Communication and Collaboration Technologies AP 4050 – WRDSB Communication Systems</i>
Revisions:	June 2019, March 2020
Reviewed:	

1. Preamble

The following procedure outlines general staff accounts, default and additional administrative computer accounts and user profiles. Guidelines and expectations regarding alterations to standard account profiles, changes in location or role of staff members and user responsibilities are also provided.

2. General

- 2.1 The board provides Personal Account Login (PAL) for access to various applications and file storage areas for the purpose of fulfilling position responsibilities and conducting board business.
- 2.2 In general but not limited to, the following are examples of applications that staff have access to: Google Suite, Trillium, accounting systems, learning applications, health and safety training applications, internal board portals and websites.

3. Default Accounts

- 3.1 All permanent and contract employees of the board are provided with a PAL account. This account is set up by the ITS department on behalf of Human Resource Services, and access and user information is provided to the employees in their new employee package.
- 3.2 All permanent and contract employees of the board are also provided with an email account within the WRDSB's Google Suite of applications. This account is set up automatically by the ITS department once employment verification is received from the Human Resource Services and entered into the HRIS system. An information package is then sent to the employee that contains user names and passwords; instructions; and procedures for the proper use of the accounts.
- 3.3 User names are created according to required formats and are based on the individual's legal name as recorded in the Human Resource Services database.

4. Additional Accounts/User Profiles

Access to additional computer applications required by individuals within the board (i.e., Finance K212, Trillium, Security Card System, Co-Op System) is provided according to predefined user profiles. These profiles are based on user roles and responsibilities for various positions within the board. For example: all head secretaries receive access to the computer applications, file storage areas and accounts they require to fulfill their job responsibilities. Similarly, all other individuals will receive access to the applications, file storage areas and accounts they need based on their position and assigned responsibilities. These accounts are set up automatically and no application process is required.

5. Alterations to Standard Account Profiles

If individuals require access to applications, file storage areas or accounts that are not part of the standard profile for that individual's role, the department, site manager or school principal can request to have these provided. They are asked to log a ticket at <https://itservicedesk.wrdsb.ca>

6. Changes in Location or Role of Staff Members

Changes required to administrative accounts due to staff members changing locations or responsibilities (i.e., administrator changing school, secretary moving from level C to level E) will occur automatically. Please refer to procedure AP 4010 Staff Devices Disposition and Account Management – Staff Change of Location or Termination of Employment with the Board for additional details.

7. User Responsibilities

- 7.1 The use of computers with access to various applications, file storage areas and accounts involves specific responsibilities by the users. These fall under three main areas.
- 7.1.1 **Account Ownership** - All computer accounts provided are for the use of the individual to whom those accounts are assigned only. Users are not to allow others to have access to their computer accounts.
- 7.1.2 **User Names and Passwords** - All computer accounts require user names and passwords. These are not to be shared with any other individuals and reasonable steps are to be taken to safeguard account passwords. Safe password management includes:
- Using a minimum of 12 characters.
 - Changing passwords if your account or password has been compromised.
 - Not using straight forward personal information as a password (i.e., middle name, child's name, etc.)
 - Not recording passwords in areas where they can be discovered (i.e., under the keyboard or desk blotter, in a day book or note pad, etc.)
- Note: Passwords that are easy for the user to recall can be created by using combinations of personal or familiar data such as part of an old phone number mixed with a special word or a favourite movie character with a number (with meaning to the user) in the middle; combining upper and lower case characters in a random manner is also very effective.
- 7.1.3 **Adherence to Board Procedures** - All use of computers and related technological equipment in the Board is governed by AP 4070 - Responsible Use Procedure for Information, Communication and Collaboration Technologies. All users are expected to know the content of the RUP and act in accordance with it.