AP I4 Information Technology Access and Security

Legislative References: *Freedom of Information and Protection of Privacy Act (FOIPPA)* section 25.1
Policy Reference: None
Collective Agreement References: none
Date: April 25, 2023

This administrative practice establishes security safeguards for appropriate use of the District's Information Technology System. These requirements are necessary to protect the integrity of the school and working environments.

Definitions

"System" means the set of technology resources that could includes a computer network, websites, hardware, and software

"User" means staff, students, contractors, or other guests of the district who may be granted access to the System.

"User ID" means the unique identifier provided by the district or the purpose of accessing district Systems

Processes

1. Individual Responsibilities
    - 1.1. The District provides access to a wide range of technological services. Users of the System are expected to:
        - 1.1.1. Comply with the District Acceptable Use of Technology Administrative Practice.
        - 1.1.2. Safeguard their passwords.
            - 1.1.2.1. Never share their passwords.
            - 1.1.2.2. Users are not to write down or store the password where others might acquire it.
        - 1.1.3. Change their passwords immediately if a User believes that it has been compromised.
        - 1.1.4. Be responsible for all activities associated with their User ID and all associated accounts.
    - 1.2. Users are not permitted to:
        - 1.2.1. Participate or engage in activities that threaten the integrity of the System.
        - 1.2.2. Connect to devices that threaten the integrity of the System.

2. User ID's and Passwords
    2.1. Individual User ID's and passwords will be assigned to all approved Users of the System by the Information Technology Manager or designate.

    2.2. Password security rules such as minimum number/type of characters will be age/grade and clearance level appropriate.

    2.3. Multifactor authentication will be implemented for users as appropriate by the Information Technology Manager or designate.

    2.4. Staff and students beyond grade 7 maintain their own passwords.

    2.5. Passwords cannot be the same as the User ID.

    2.6. Passwords will expire as needed to maintain security.

    2.7. Use of any User ID and/or password combination other than the user's own is not permitted.

    2.8. Users may be given different levels of System access as appropriate.

    2.9. User accounts and access will generally expire concurrently with the resignation or termination of an employee or upon a student's withdrawal from school.

3. Software and Equipment
    3.1. Only District authorized software and equipment will be maintained on the System.
        3.1.1. Software not provided by the District require prior authorization from the Information Technology Manager before they can be used on the System.

    3.2. Unauthorized software that is found on the System will be blocked or removed.

    3.3. Modification of the System is strictly prohibited unless it has been approved by the Information Technology Manager.

    3.4. All new software/app requests will follow the process set out in the District Approval of Software and Apps Practice.

    3.5. All school-based software, prior to purchase, must be assessed for compatibility, redundancy, educational/business merit, and privacy compliance.

3.6. All school-based software will be procured and appropriately licensed by the Information Technology Manager or designate.

3.7. All school-based purchased hardware, prior to purchase, must be assessed for compatibility and procured by the Information Technology Manager or designate.

3.8. Users must not unplug, disconnect or otherwise change any wiring in the System unless such a change has been approved by the Information Technology. Manager or designate.

4. Network Backup, Storage and Printing

4.1. Users are responsible for having a current backup of their data.

4.2. The District is not liable for any loss of data.

4.3. Network storage will be monitored.

4.4. The Information Technology Manager reserves the right to move/delete any file to protect the integrity of the System.

4.5. Only District approved network printers will be connected to the Intranet.

5. Communication

5.1. All staff are required to use the electronic communication address(es) provided by the District for all professional communications related to their employment with the District.

5.1.1 District electronic communication addresses should not be used for personal communications.

5.2. Sending/redirection of user email to third party services (such as Hotmail, G-mail, Yahoo, etc) may not be configured.