SECURITY SAFEGUARDS

Background

This document 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.

Procedures

1. User ID's and Passwords:

   1.1. Individual User Id's and passwords will be assigned to all Users of the "System".

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

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

   1.4. Passwords will expire yearly or as needed to maintain security.

   1.5. Use of any User ID and/or password combination other than your own is not permitted.

   1.6. Users may be given different levels of "System" access appropriate to their educational needs.

2. Software and Hardware:

   2.1. Only District authorized software and equipment can be used on the "System".

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

   2.3. Software and/or devices not provided by the District require prior authorization from the District's Director of Information Technology before they can be used on the "System".

   2.4. Hacking is strictly prohibited

   2.5. Modification of the "System" is strictly prohibited unless it has been approved by the District's Director of Information Technology.

   2.6. All school based purchased software that needs to be installed on the "System" must be appropriately licensed and checked for compatibility by the District's Information Technology Department personnel before it is installed on the "System".

   2.7. All school based purchased hardware that needs to be connected to the "System" must be checked for compatibility by the District's Information Technology Department personnel before it is connected to the "System".

3. Printing, Network Storage and Backup:

   3.1. Network storage and printing usage will be monitored and reports will be available to each school.

   3.2. The District's Director of Information Technology reserves the right to move/delete any file to protect the integrity of the "System".

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

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

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

4. Power/Cost Saving:

4.1. All non-essential technology hardware will be turned off or placed into a power saving mode when not in use.

4.2. Printers that are duplex capable will be set to duplex by default.

5. Communication:

5.1. All staff are required to use electronic communication that is provided by the District.

5.2. Inappropriate communication is prohibited.

5.3. Sending/redirection of summer.com user email to third party services (such as Hotmail, G-mail, Yahoo, etc) will not be configured by the District's Information Technology Department personnel.

6. Individual Responsibilities

6.1. The District provides access to a wide range of technological services. "Users" of the "System" are expected to:

6.1.1. Comply with the District Acceptable Use of Technology Administrative Procedure.

6.1.2. Safeguard their password.

6.1.3. Never share their password. Users are not to write down or store the password where others might acquire it.

6.1.4. Change their passwords immediately if a "User" believes that it has been compromised.

6.1.5. Be responsible for all activities associated with an individual's User's log-on.

6.2. Users are not permitted to:

6.2.1. Participate or engage in activities that threaten the integrity of the "System".

6.2.2. Connect to devices that threaten the integrity of the "System".

6.2.3. Unplug, disconnect or otherwise change any wiring in the "System" unless such a change has been approved by the District's Director of Information Technology.

7. Change

7.1. As the integrity of the District's technology systems are critical, measures to safeguard those systems will be updated from time to time as required by the District's Director of Information Technology.

Reference: Reference: Sections 17, 20, 22, 65, 85 School Act
Freedom of Information and Protection of Privacy Act
School Regulation 265/89
Canadian Charter of Rights and Freedoms
Canadian Criminal Code
Copyright Act
Introduction to British Columbia's Redesigned Curriculum, 2015