DISTRICT INFORMATION TECHNOLOGY SERVICES

Background

The District is committed to providing students and employees access to information technology services (ITS) for success in life and work in the 21st Century. These goals are enhanced by the provision of such services. This procedure shall govern the use of all information technology services and devices.

Procedures

1. Definition

   1.1. Information Technology Services (ITS) refers to all computer and computer-related hardware, software, the local and wide area networks and servers, peripherals, handheld devices, all digital communication devices, and operating systems. Appropriate internet access and communication tools are provided by the District to students, employees, contractors, and others.

2. General Access and Usage

   2.1. Access to systems is granted by the District. Access to ITS is a privilege, not a right. Staff, students, parents, and educational partners using ITS resources are therefore expected to do so in a responsible, ethical manner, in observance of the District's intentions set out in this procedure.

   2.2. Guest wireless access will be provided only after accepting a terms of use agreement. Non-District peripheral, mobile or personal devices, must not interfere with the function of the network or its security.

   2.3. The District reserves the right to inspect and remove electronic devices connected to ITS networks for inappropriate use or for files or software that threaten the operation of the network.

3. Bring Your Own Device (BYOD)

   3.1. Definition:
       3.1.1. All portable, wireless (including cellular devices such as small tablets, gaming, and handheld) devices using mobile operating systems and other electronic devices that facilitate communications (either verbal, visual, or text), including personal laptop computers.

3.2. Device owners agree to:

3.2.1. Install anti-virus software and ensure that virus recognition data files are updated on a continuous basis.

3.2.2. Install anti-spyware software and ensure that spyware recognition data files are updated on a continuous basis.

3.2.3. When announced by software vendors, consider installation of all currently security patches and software updates.

3.2.4. Adhere fully to the SD47 Acceptable Use Administrative Procedure and understand that computer and networks usage will also be governed by school and classroom rules and expectations.

3.2.5. Strictly ensure that software installed on their privately-owned device(s) are licensed for their use.

3.2.6. Give their computer a machine name that is acceptable to the District.

3.3. The District agrees to:

3.3.1. Provide internet access for personal devices.

3.4. The District is NOT responsible for:

3.4.1. Repair of privately-owned devices (hardware or software).

3.4.2. Compatibility problems with its networks, devices, and software.

3.4.3. Network connectivity problems.

3.4.4. Theft or damage of privately-owned devices, software, or data.

3.4.5. Providing licenses for software use on privately-owned devices.

4. Liabilities

4.1. The District does not guarantee that the functions or services performed, or that the information or software contained on the ITS will meet the ITS user's requirements, or that the ITS will be uninterrupted. Users are encouraged to back up personal data to external storage devices or cloud services and to save electronic correspondence to a personal computer, external storage device or cloud service to prevent data loss.

4.2. The District assumes no responsibility or liability either directly or indirectly for any personal use or personal costs which are incurred when using the ITS. The opinions, advice, services, and all other information expressed by ITS users, information providers, service providers or other third-party individuals in the District's ITS and on the Internet are those of information providers and not the District.

4.3.   The District makes no warranties of any kind, whether expressed or implied, for the service it is providing, or quality or accuracy of information obtained through its services. The Board will not be responsible for any damage users may suffer including loss of data or service interruptions or problems caused by user errors. The District is not responsible for maintaining or updating personal devices or for keeping them in working order. Use of any information obtained via the internet is at the user's risk.

5.   Privacy and Confidentiality

5.1.   Users are expected to respect all guidelines from the Freedom of Information and Protection of Privacy Act to ensure that personal information is not compromised in public areas.

5.2.   The use of the ITS, including Internet access, is neither private nor confidential and may be tracked or archived. Use of the ITS, including the Internet, by any individual may be monitored or reviewed by the Superintendent without prior notice if there are reasonable grounds.

5.3.   The Superintendent may remove locally posted communication that is unacceptable. ITS users cannot copy or post messages to public areas without the consent of the specified user and complying with content guidelines of this procedure.

5.4.   In accordance with the provincial Freedom of Information and Protection of Privacy Act the Powell River District will not intentionally inspect the contents of users' e-mail, or disclose the contents to anyone other than the sender, or intended recipient, without the consent of the sender or intended recipient, unless required to do so by law or the policies of the Board.

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

Adopted: August 26, 1997
Reviewed: June 21, 2016
Revised: May 18, 2022