POLICY 122 DIGITAL CITIZENSHIP

The Board of Education of School District No. 83 (North Okanagan-Shuswap) supports the use of information technology for educational purposes and believes that, if used effectively, information technology is a means to improve student learning.

This policy is provided to ensure that all users of district networks are aware of their responsibilities for acceptable use of all district networks and that the communications between the school district network and the Internet may be blocked and/or decrypted to support a safe, secure, and robust network.

As all access to the Internet through the school district network is intended to support the goals, objectives, and activities of the school district and the district strategic plan it is essential to inspect Internet traffic to verify its security, legitimacy, veracity and application.

The Board of Education recognizes the benefits of providing district networks to its users; however, the Board is also aware of the risks involved. School District No. 83 (North Okanagan-Shuswap) will decrypt or block Internet traffic for all devices connected to the school district network in accordance with the guidelines outline below. This policy will apply to all devices connected to the school district network and users of these devices need to recognize the need to block and/or perform decryption on Internet traffic to reduce the risk to the Board by ensure a safe, secure and robust network.

School District No. 83 (North Okanagan-Shuswap) will conduct security training awareness campaigns to hone employee and student security skills to reduce the risk of a potential security breach.

Guidelines

1. Definitions

- "Digital Citizenship" is defined as appropriate, responsible behaviour with regard to technology use.
- "Digital Footprint" is the data trace or trail left by someone's activity in a digital environment.
- "Appropriate use" is based on community standards and includes school district expectations.
- "Excessive use" is based on the time, capacity, and accessibility of resources of a particular user.
- "Inappropriate use" includes, but is not limited to accessing pornography, hate literature, illegal or offensive material, or anything that contravenes the B.C. Human Rights Act or the Freedom of Information and Protection of Privacy Act or Copy Write Laws.
- "Independent" refers to the supervised access of networks, including the Internet, of which the school district does not have direct control. This includes, but is not limited to, personal electronic mail.

Adopted: June 2012
Amended: June 2019

- "Internet" is defined as electronic resources over which the school district does not have direct control.
- "Network" refers to any electronic method of communications. This includes, but is not limited to computer-based data systems and video-conferencing.
- "Wi-Fi" refers to the establishment of a wireless computer network within school and district buildings for the purpose of connecting to the district communication and information technology network.
- “Decrypt” refers to a method used to provide access to the packet data so that traffic may be inspected.

2. Acceptable Use of Networks

2.1. The purpose of communication and information technology networks is to support communications, research, education, and the achievement of school and district goals and objectives.

2.2 Internet traffic that fits into the following URL categories as defined by the provincially chosen network vendor will not be decrypted. The District does not decrypt financial services.

2.3 Internet traffic that fits into the following URL categories defined by the provincially chosen network vendor list of URL Categories will be blocked: Adult, Nudity, Malware, Phishing, Peer-to-Peer.

2.4 All digital content (including email messages) created or stored in any of the school district systems are the property of School District No. 83.

2.5 All content stored, sent or received within any school district systems is subject to the Freedom of Information and Protection of Privacy Acts.

2.6 Users are expected to follow storage and retention policy with respect to electronically stored data. (This policy is in process – fixed rules are coming).

2.7 Users of networks, including the Internet, must follow these acceptable rules of network behaviour and etiquette. Specifically, users must not:

2.7.1 Use networks, including the Internet for their own commercial gain.

2.7.2 Use networks, including the Internet, for inappropriate and/or unlawful purposes.

2.7.3 Access and/or place inappropriate, pornographic or unlawful information on networks, including the Internet.

2.7.4 Use abusive, sexist, profane, racist and/or other objectionable language in any electronic communications.

279.5 Use another user’s identification and/or password or attempt to harm or destroy the data of another person.

2.7.6 Circumvent security measures and/or access areas and services to which the user is not authorized.

2.7.7 Use network facilities and resources in an excessive and/or inappropriate manner. This may include but is not limited to, network intensive games.

2.7.8 Break copyright laws.

2.7.9. Access to trending social media apps, for personal use.

2.8 It is the responsibility of all users to inform themselves of the specific application of these acceptable and restricted uses of networks and the Internet. Failure to comply with these

rules may result in disciplinary action through established procedures in statutes, collective agreement, student codes of conduct and school district policy.

3. Use of Electronic Personal Devices

3.1 These guidelines and policies apply to the use of all laptop computers and all other mobile internet-capable devices. No personally owned device will be connected to the hard-wired School District Network.

3.2. The School District will not be held responsible in any capacity for physical damage, loss or theft of any personally-owned device.

3.3. Use of personally-owned devices in the classroom will be at the discretion of the classroom teacher. Personal devices must be part of a respectful learning environment and must meet the needs of the classroom. Classroom teachers may prohibit, restrict or regulate use of personally-owned devices.

3.4. All use of a personally-owned device must support the instructional activities currently occurring in the school environment.

3.5. Devices with camera and video capability must not be used without consent of the person(s) being photographed.

3.6. Personally-owned devices may be used for instructional purposes and for managing medical situations or emergencies.

3.7. Employees, guests, students and their families accept that their personally owned devices may be remove from the network if it is not found to be in compliance with school and district codes of conduct, policies and guidelines, including the Digital Citizenship Acknowledgement/Agreement and the requirements of the provincial network. Students and their families also accept that school authorities may inspect the device and its contents to also ensure compliance.

3.8. All users access the network at their own risk. The school district will not be held responsible for damage that may occur as a result of connecting to the network or any electrical power source.

3.9. All users bringing personal technology to school are responsible for and will be required to reimburse the School District for any damage that may be caused through the use of network with his/her personally-owned device.

4. Consequences

4.1. Failure to comply with these guidelines and policies may result in disciplinary action by the school which may include, but is not limited to, loss of access to the network and other school district discipline.

Adopted: June 2012
Amended: June 2019