A Guide to using VSB Wireless Networks

The VSB Learning and Information Technology (LIT) Division is pleased to provide three wireless networks for use at schools and other District locations. These networks are designed and meant to be used for educational and VSB business purposes and each supports a specific type of need. A variety of wireless devices can connect to these networks including Windows laptops, tablets, and phones, Mac laptops, iPads, iPods, iPhones, Android devices, LCD Projectors, and Apple TVs. Whether these devices are owned by VSB, individuals, or have been donated to schools, they can connect.

VSB-Secured
This network is designed for devices that support the ability for users to login with their VSB user-id and password, and logout when necessary. There are no restrictions imposed on bandwidth or what online services can be accessed. Devices that fit this network use include:

- Windows laptops and tablets (owned by the VSB)
- Mac laptops (owned by the VSB or the individual)
- iPads, iPods, iPhones, Windows Phones, Android phones and tablets (used by an individual only)

VSB-Visitors
The VSB-Visitors network is designed for people who are not employees or students of VSB, i.e., people who do not have a VSB user-id and password. However, as an interim measure, personally owned Windows laptops also must use this network until the VSB has an automated system to check for up-to-date anti-virus software and confirmation the computer has current software updates installed. Once the VSB is able to implement a means to automate this, personally owned Windows laptops will be able to safely use the VSB-Secured network. This measure is designed to protect both the network itself and other wireless users. This network has an imposed bandwidth limit of 1mbps and only provides access to District and Internet web-based sites and content.

A passphrase (aka a pre-shared key) is required to connect to this network. The passphrase is changed monthly by the LIT Service Desk. Upon change, the passphrase is emailed to school offices, the education centre receptionist, and posted on the front page of myVSB.

VSB-Commons
The VSB-Commons network is designed for devices or appliances (e.g., Apple TV, Printers, Projectors, etc.) that are not able to login to the network with a userid and password. It is also designed for shared Tablet use (e.g., student iPads) where multiple people will use the tablet. These devices are configured by the school technician. Network access is enabled through the use of security keys, which do not expire, embedded into the device(s) configuration.
Learning Benefits and Appropriate Use

With wireless access come new responsibilities and likely distractions for students and staff. Schools are advised to have conversations with teachers and teachers with their students about the new capabilities. It is important to discuss the benefits to learning and productivity while addressing the concerns around inappropriate use and distractibility. The District has nearly completed its work on new acceptable use and social media policies and regulations. This work will further guide the safe and productive use of technology in schools and other VSB work places.

Digital tools often amplify behaviors that are already in place. It is important that schools have conversations about the new digital access that is possible anywhere on any device at any time, in the context of adhering to current school codes of conduct and social responsibility expectations.

Increasingly, students are bringing their personal technology (smart phones, handhelds, tablets, and laptops) to school. With some exceptions, current practice at most schools is to ask students to put their technology away when they are in class. In 2013, the District intends to form a focus / study group to work with a select few secondary and elementary schools to develop guidelines to assist schools in transitioning to a new practices where students are encouraged to bring their own technology to use for learning. The resulting guidelines will assist teachers, principals, and students in engaging productively with powerful personally owned learning devices while wirelessly connected in classrooms and other spaces in their schools.

For the interim, some statements that should guide these conversations in schools include:

**Student Rights**
- Privacy of personal information including pictures, videos, and comments about them
- Use their devices to support their learning
- To feel safe and be respected

**Student Responsibilities**
- Take responsibility for their choices and actions
- Learn about the risks of sharing their personal information including images, birthdates, where they live, phone numbers, the school they attend
- Not use someone else’s identity (eg, password)
- Not take pictures or record videos of others on school property without their permission
- Seek out content that is of educational quality and that will help their learning
- Acknowledge and respect the ownership others have over their work
- Limit personal use, not related to their learning, of the network (eg, watching videos, listening to music, downloading files, Facebook, etc.)
- Learn about and understand how their actions with their technology can affect others or be perceived as offensive
- Protect their passwords
- Ensure their actions do not damage District resources (eg, no viruses, hacking)
- Respect the rights and freedoms of others
Not hurt or mistreat others by what they create and share including pictures or videos
- Do not harass, stalk, threaten, insult, or attack others
- Report unsafe and inappropriate behavior to their teachers or school Principal

**Teacher Rights**
- Privacy of personal information including pictures, videos, and comments about them
- Use their devices to support their learning
- To feel safe and be respected

**Teacher Responsibilities**
- Keep their students’ personal information including pictures and videos private unless parents provide consent to share
- Model the ethical use of information
- Seek out content that is of educational quality that will help their students learn
- Teach their students how to locate, evaluate, and use information
- Model and teach digital responsibility in their classroom and school
- Ensure that students feel safe, are protected and respected online within their classroom activities
- Facilitate student learning about appropriate behavior online
- Report behavior that is harmful, unsafe, or inappropriate (eg, harassment, stalking, threats, insults, or attacks)

**Conversation resources:**
- LearnNowBC Cybersafe Resources - [http://www.learnnowbc.ca/inbresources/cybersafe/](http://www.learnnowbc.ca/inbresources/cybersafe/)
- Erase Bullying - http://www.erasebullying.ca/
- Copyright Matters! Some Key Questions & Answers for Teachers [http://cmec.ca/Publications/Lists/Publications/Attachments/291/Copyright_Matters.pdf](http://cmec.ca/Publications/Lists/Publications/Attachments/291/Copyright_Matters.pdf)