Newfoundland & Labrador English School District

Policy:	ACCEPTABLE USE OF TECHNOLOGY	FIN-500
Division:	FINANCE AND ADMINISTRATION	
Cross Reference:	FIN-501 – EMAIL FIN 502 – SOCIAL MEDIA USE	

ADMINISTRATIVE PROCEDURES / REGULATIONS

1. General
   - 1.1. Technology resources are intended for educational purposes and for conducting business operations of the District.
   - 1.2. Use of technology resources must support student achievement and be consistent with the mission and goals of both the District and schools.
   - 1.3. Users are expected to follow the same rules for good behavior and respectful conduct online as they conduct themselves offline.
   - 1.4. The District will take all reasonable steps to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of District technology resources.
   - 1.5. Users are expected to alert school administration, supervisor, or the Information Technology Department of any concerns regarding misuse, safety, privacy or security of District technology resources.
   - 1.6. Use of technology resources is subject to all policies, regulations and practices of both schools and the District as it relates to technology, property and conduct.
   - 1.7. Users with access to personal and/or confidential data are to utilize all appropriate precautions to maintain the accuracy, integrity, and confidentiality of the data and ensure that no unauthorized disclosures occur.
   - 1.8. Limited personal use of technology resources is permitted provided the use does not:
     - 1.8.1. Violate this or another District/School policy or regulation;
     - 1.8.2. Interfere with staff productivity;
     - 1.8.3. Interfere with the business operations of the NLESD;
     - 1.8.4. Interfere with IT operations; or
     - 1.8.5. Compromise the NLESD in any way.

2. Use of Personal Devices in the District

   If a user chooses to bring their own personal electronic/computing device and connects to the District's network, the Acceptable Use of Technology Policy is still applicable, as well as the following:
   - 2.1. Personally owned devices are not to be connected to the District's network if any file-sharing applications (Peer-to-Peer – P2P) such as, but not limited to, Limewire, BitTorrent, uTorrent, Shareaza, etc. are present. Such applications must be completely removed from the device, and not just simply disabled, before connecting to a school or District network.
   - 2.2. Users that connect their personally-owned device to the District's network must ensure that their device is password protected.

2.3. Users are responsible for the security, care and maintenance of their own device.
2.4. Users must ensure their device is protected by an enterprise antivirus/anti-malware application such as Symantec, Microsoft, MacAfee, etc.
2.5. Users are fully responsible for the personally owned devices while it is at school. The District is not responsible for the loss, theft or damage of the device.
2.6. Personal devices (e.g. student-owned iPads, cell phones, laptop computers) are permitted in schools, in accordance with consistent, school-wide guidelines as determined by the school administration and staff.
2.7. The use of personal devices in the classroom should be for educational purposes only, in accordance with consistent, school-wide guidelines and practices as determined by the school administration and staff.
2.8. Inappropriate use of personal devices/technology will result in consequences, as outlined in the Acceptable Use of Technology Agreement – Students and Parents/Guardians: https://www.nlesd.ca/includes/files/policies/doc/1525974023153.pdf.
2.9. In general, the use of personal devices is not permitted in K-6 classrooms, except in circumstances where their use is required to support the documented learning needs of individual students. This determination is made by the school administration, in consultation with appropriate staff.

3. Security
3.1. Users must not download or attempt to download or run unauthorized applications over the school network without express permission from the Information Technology Department.
3.2. Users must not introduce, create, or propagate any malicious programs, including, without limitation, viruses, worms, Trojans, spyware, or other malicious code, to any District system.
3.3. If a user believes that a computer is infected with a virus, or malware, you are to stop using the system immediately and report the incident to a school administrator or Information Technology Department right away.
3.4. Users must not attempt to remove the virus or malware or download any programs to help remove the virus or malware.
3.5. Users must not tamper with any hardware, networks, applications, network systems, computers or other users' files without authorization or permission. In particular users must not:
- Attempt to gain unauthorized access to District/school/other's data;
- Attempt to vandalize the District's systems;
- Circumvent or alter software, physical protections or other technology restrictions placed on computers, networks, software, applications or files, including District-installed virus protection software; or
- Launch attacks or probes, or otherwise attempt to subvert the security of any system or network.

4. Internet Access
Using a web browser to access the Internet can potentially expose end-users to inappropriate material and other objectionable content. To combat exposure to such threats, the District filters web sites believed to be inappropriate as a security strategy to protect users while online.
4.1. Users are expected to regard the web filter as a safety and security safeguard, and under no circumstances should users try to circumvent it when browsing the Internet.

As no filtering system is perfect, the District cannot, and does not, guarantee that inappropriate or objectionable material can be completely filtered.

5. Passwords

Usernames and passwords (access ID) help ensure the security and confidentiality of data that is stored on various systems and servers across the District. It is your responsibility as a user, to make sure that all your account passwords are as difficult to guess as possible.

5.1. All passwords used within the District must meet strong password requirements and have characteristics that follow the format below:

5.2. Passwords must meet the following minimum character requirements:

- Be at least eight characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters (for example,!, $, #, %)

5.3. Never write down your password as a means to remember it.

5.4. Some systems will assign a default password to a user to gain access. This password must be changed immediately when the user is logging in.

5.5. Users are responsible and accountable for all activity that occurs within their password protected account(s).

5.6. When completed work, users must log off each password protected account.

5.7. If you suspect tampering with a network password notify a school administrator, supervisor or call the Information Technology Department immediately.

5.8. Users are responsible for the security and safeguard of any assigned password protected accounts (username and password).

5.9. Under no circumstances is a user to share their assigned login information with another user or login using another user's username and password.

6. Transportation of Personal and/or Confidential Information

6.1. Use of unencrypted CDs, DVDs or portable USB drives to transport confidential or personal information is prohibited.

6.2. Transporting personal or confidential information must be done using an encrypted device (e.g. encrypted USB drive, encrypted volume on a laptop).

6.3. Users should limit the amount of personal and/or confidential information being transported or taken home. For example, just take the student name and not other student identifying information.

6.4. Users should transport personal information **only when necessary,** and do not leave the information on the device afterwards.

7. Unauthorized Network Devices

Network devices such as wireless access points, switches, routers, hotspots, etc. that are not authorized, not installed and not configured by the District's Information Technology staff are considered rogue devices, and represent an open and unsecure entry point into our network. Such rogue devices can circumvent network security and expose the network to security threats.

7.1. Extending a District or school network by introducing a rogue device such as wireless access point, switch, router, hotspot, or any other service or device is strictly prohibited.

8. Unacceptable Use

8.1. Participating in any illegal act or breaking any local, provincial or federal laws.

8.2. Duplicating, storing, or transmitting pornographic or objectionable materials.

8.3. Using the District's network and/or the Internet for illegal or criminal or online gambling or other inappropriate purposes, or in support of such activities.
8.4. Accessing, reviewing, uploading, downloading, storing, printing, posting or handing out material or content that is criminal, illegal, inflammatory, discriminatory (hate literature), abusive, obscene, rude, vulgar, profane, sexually graphic, supports violence or is harassing/bullying/threatening.
8.5. Unlawful/unauthorized duplicating, installing, storing or transmitting copyrighted material;
8.6. Posting information that is false, insulting or is a personal attack about a person.
8.7. Logging into a computer system using another user's account information.
8.8. Using unauthorized file sharing applications or illegally downloading or sharing files, including, without limitation, movies, music, applications, and other software.
8.9. Peer-2-Peer (P2P) applications such as, but not limited to, Limewire, BitTorrent, uTorrent, Shareaza, etc. are strictly prohibited.
8.10. Using the District's network for commercial, financial, or political purposes or other related personal gain.
8.11. Installing software of any type onto computers without the direct permission of the Information Technology Department.
8.12. Sharing or posting personally identifiable information including but not limited to: address, phone number, or picture that has not been authorized.
8.13. Destroying, damaging or disabling any computer equipment (hardware or software).
8.14. Attempting to gain access to someone else's information or account without permission.

9. Violations

Violations of these regulations may result in access relating to District technology being restricted, suspended, or revoked and may result in disciplinary action.

Violations of this policy may be reported to the appropriate law enforcement authorities and may also be subject to criminal investigations and/or criminal charges. Users are also advised that inappropriate use could result in:

1. Criminal prosecutions under the Criminal Code and other Canadian or Provincial laws.
2. Civil actions where appropriate (e.g., intentional damage to the computer network, computer hardware, software, etc.).

10. Disclaimer

District technology services and information systems are provided on an "as is", "as available" basis. The District makes no guarantees, or warranties of any kind, whether express or implied, about the reliability and availability of the technology it provides and will not be responsible for any damages that may be incurred as a result of use of any District technology. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by technology or user errors or omissions. Use of any information obtained or given via the Internet or email is at the user's risk. The School District denies any responsibility for the accuracy or quality of information obtained through its technology services.