NLSchools refers to all public K-12 English schools and school-related facilities under the jurisdiction of the Department of Education, Education Operations Branch and all employees working therein providing services and supports to such schools, including those who work in the areas of school facilities, student transportation, program implementation, student services, and procurement.

Policy Name

Acceptable Use of Technology

Policy Statement

The Department of Education supports the use of information and communication technology (ICT) for instructional programs, in order to facilitate teaching and learning through interpersonal communications; access to information; research and collaboration; and, to support the business functions of the public school system. The department is committed to providing an accessible, reliable and secure technology environment for staff, students and guests for the purposes of teaching, learning and administrative use.

The Department of Education acknowledges that the need to protect the integrity of all ICT systems and the security, privacy and safety of all students and staff is of paramount importance. As such, the department requires acceptable, ethical, legal and responsible use of all ICT systems.

Background

The Department of Education recognizes the value and need for technology in the educational setting and therefore provides staff and students within NLSchools with access to ICT systems, which includes Internet access. In support of this, NLSchools invests significant resources in the purchase, development, and utilization of ICT systems for both teachers and students. The IT staff for NLSchools will provide education and awareness for staff and students in the responsible use of technology.

Incorporating technology into everyday classroom practices enhances the learning environment for students, as it supports the acquisition of skills in literacy, numeracy, and higher order learning. Within the context of its mission and vision, the ICT systems assist in preparing students for success in life and work in the 21st Century.

These technology tools, used appropriately, provide global information resources,

opportunities for collaboration and communication, and media-rich teaching and learning experiences for students and teachers.

Scope

This policy is applicable to all students, staff and authorized users of the ICT systems within NLSchools.

Definitions

For purposes of Acceptable Use of Technology Policy:

ICT

ICT is an acronym for "Information and Communication Technologies." It refers to technological tools and resources used to communicate, and to create, distribute, store, and manage information. These technologies include, but are not limited to, all of the computer hardware, operating system software, application software, stored text and data files. This includes, but is not limited to, electronic mail, local databases, externally-accessed databases, desktops/laptops, recorded magnetic or optical media, clip art, digital images, digitized information, and communication technologies and hardware, etc.

Internet

The internet is a single worldwide computer network that interconnects other computer networks, on which end-user services, such as World Wide Web sites or data archives, are located, enabling data and services to be accessed and exchanged.

Authorized User

An authorized user is an individual who is approved and has been given specific permission(s) to use or access a particular technology resource such as computers, computer-related devices, data bases, email and other technology related resources. The amount of access to technology resources and networks will be determined by function and need by designated public school system personnel in partnership with the OCIO executive.

Monitoring of Electronic Communications

Monitoring of electronic communications refers to the use of a mechanism such as

firewalls, web filters, etc., to access, review and subsequently analyze activity, information or use of any ICT system or network.

Policy Directives

1. Each school shall incorporate the Acceptable Use of Technology policy and administrative procedures into their school practice.

2. All authorized users must sign an Acceptable Use of Technology Agreement, which defines access, expectations of use and penalties/consequences of improper use.

3. The Department of Education and its agents, have the right, but not the obligation, to monitor any and all technology use to ensure compliance with expectations set forth in this policy.

4. The department retains the right to access, inspect, investigate and monitor all use and its resources, including all data files, communication networks and information created on, with or transmitted using its ICT resources, and including e-mail, text messages, internet usage, and any other communications or information. All such files, communications, or information may be monitored, reviewed and/or accessed by personnel who are authorized to do so and have an appropriate reason pursuant to civil and criminal matters, investigatory purposes, or any other lawful reason, including but not limited to the following:

    a) There are reasonable grounds to suspect abuse, non-compliance with policy/ procedures, or improper or illegal activities.

    b) It is required by subpoena or court order.

    c) It is required in order to respond to an access to information request or suspected privacy breach under the Access to Information and Protection of Privacy Act (ATIPPA).

    d) It is necessary to conduct an audit or ensure the security and operating performance of ICT resources.

    Monitoring and searches, if required, will be carried out by a staff person as designated by the Superintendent of Schools.

5. The department reserves the right to block, limit, or disallow any application, website, address, or protocol deemed inappropriate and/or that place a burden upon the ICT infrastructure.

6. Users of NLSchools ICT infrastructure are expected to behave as they would in any other environment where they represent their school. Users are to conduct themselves in a responsible, ethical, and respectful manner.

7. The ICT systems are provided to enhance the delivery of educational programs and related support services and for conducting other school business.

Administrative Procedures

1. General

    1.1. Technology resources are intended for educational purposes and for conducting business operations of NLSchools.

    1.2. Use of technology resources must support student achievement and be consistent with the mission and goals of both NLSchools 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 department 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 NLSchools technology resources.

    1.5. Users are expected to alert school administration, supervisor, or NLSchools Information Technology Division of any concerns regarding misuse, safety, privacy, or security of technology resources.

    1.6. Use of technology resources within the schools are subject to all policies, regulations and practices of both schools and NLSchools 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 NLSchools/School policy or regulation;

        1.8.2. Interfere with staff productivity;

        1.8.3. Interfere with the business operations of NLSchools;

1.8.4. Interfere with IT operations; or

1.8.5. Compromise NLSchools in any way.

2. Use of Personal Devices on NLSchools Network

If a user chooses to bring their own personal electronic/computing device and connects to NLSchools 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 NLSchools 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 NLSchools network.

2.2. Users that connect their personally-owned device to NLSchools 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 device while it is at school. NLSchools 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: see related documents for this policy.

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 NLSchools Information Technology Division.

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 NLSchools 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 NLSchools Information Technology Division 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 NLSchools/school/other's data;
- Attempt to vandalize NLSchools systems;
- Circumvent or alter software, physical protections or other technology restrictions placed on computers, networks, software, applications or files, including Government-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, NLSchools 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, NLSchools 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 public school system. 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 NLSchools 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 NLSchools Information Technology Division 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 NLSchools Information Technology Division 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 an NLSchools 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 NLSchools 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 NLSchools 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 NLSchools Information Technology Division.

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 NLSchools 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

NLSchools technology services and information systems are provided on an “as is”, “as available” basis. NLSchools 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 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. NLSchools denies any responsibility for the accuracy or quality of information obtained through its technology services.