



Northwest School Division #203

Computer Network Acceptable Usage Policy

Purpose: This policy guides users of the Northwest School Division's Information Technology (IT) infrastructure. It balances the employee's ability to benefit fully from information technology with the School Division's need for secure and effectively allocated IT resources.

Background: The increasing use of information technology has fundamentally changed the workplace. The Internet, intranets, cellular telephones, fax machines and e-mail have transformed data management and communication and employees utilize this valuable resource in many innovative ways.

The networked office has also created the opportunity to access material and use resources in ways that may not be acceptable. Inappropriate use of information technology could expose the Northwest School Division to potential embarrassment and possible litigation. The Northwest School Division is committed to ensuring that this valuable resource is not brought into disrepute in the workplace through inappropriate use. Employees are to follow this policy to ensure that their own use of the school division's information technology resources is appropriate.

Policy: Employees of the Northwest School Division will follow guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations and policies. The Northwest School Division will periodically redefine and enhance these guidelines and policies. This policy addresses circumstances which are new and evolving, or at least unfamiliar. It augments, rather than replaces, existing Northwest School Division policies.

The use of NWSD technology, including Internet access, is a privilege, not a right. All users are expected to act and behave in a manner appropriate for an educational institution.

Employees who violate this policy will be subject to a full range of disciplinary actions.

There are three usage types for the Northwest School Division infrastructure:

- Acceptable,
- Incidental and
- Unacceptable.

The chart contained in Appendix "J" of this policy provides examples of these three usage types and may be used as a guideline when assessing use of information technology.

The appendices discuss specific applications such as the Internet and e-mail in more detail.

- Appendix 'A' -Internet Use
- Appendix 'B' -E-mail
- Appendix 'C' -Games
- Appendix 'D' -Notebook Computers
- Appendix 'E' -Remote Access Services
- Appendix 'F' -Anti-Virus

- Appendix 'G' -File Sharing
- Appendix 'H' -Acceptable/Incidental/Unacceptable Usages

Acceptable

Acceptable uses are activities required to conduct the businesses of education and libraries. They help fulfill the mandates set forth by School Divisions, Post Secondary Institutions, Libraries and Saskatchewan Learning.

Acceptable use is any application used in the delivery of services by education partners which does not disproportionately consume available resources.

Incidental

Incidental uses are those that are neither explicitly permitted nor explicitly denied. Incidental usage that becomes an imposition on others or burdens systems is no longer incidental, but unacceptable, and is not permitted.

Unacceptable

Unacceptable use impedes the work of others and may unintentionally damage the infrastructure. Unacceptable usage may generate extra costs for the Northwest School Division (NWSA).

It is unacceptable to:

- Use, copy, or otherwise access anyone else's files without authorization.
- Use the NWSA information technology infrastructure for activities that contravene the law, existing policies or regulations.
- Use any part of the NWSA information technology infrastructure for personal financial gain.
- Infringe copyright or proprietary rights.
- Permit unauthorized access.
- Create or propagate computer viruses.
- Damage files, equipment, software, or data belonging to others.
- Use or attempt to use unauthorized access methods or abilities.
- Compromise the privacy of users and their personal data.
- Damage the integrity of a computer system, or the data or programs stored on a computer system.
- Bring the Northwest School Division into disrepute.
- Disrupt the intended use of system or network resources.
- Put unjustifiable demands on Community Net's infrastructure
- Facilitate unauthorized access attempts on other computer systems.
- Result in the uploading, downloading, modification, or removal of files on the network for which such action is not authorized.

The above list is not exhaustive.

The NWSA infrastructure provides access to outside networks. Users may encounter offensive or objectionable material. The NWSA does not assume responsibility for the content of any of these outside networks. Without specific authorization, users must not cause, permit, or attempt any installation of hardware or software, destruction or modification of data or equipment that will affect other users of the NWSA infrastructure.

Monitoring:

Users should be aware that computer usage can be traced by site logs and other tracked information. The Northwest School Division reserves the right to access the contents of all files stored on its systems and all messages transmitted through its information technology infrastructure.

Application:

This policy applies to all users who subscribe to services provided through the Northwest School Division infrastructure.

Appendices

Technology changes rapidly and its use varies widely within Northwest School Division. For example, a few years ago personal digital assistants (PDAs), networked photocopiers and workstations with worldwide Internet access were unheard of. Now, they are becoming commonplace in many offices. The list of applications and devices in these appendices is therefore illustrative, not exhaustive. It represents a baseline for acceptable usage and may be used as a template for Northwest School Division-specific policies.

Appendix "A"

Internet Use

Users who access the Northwest School Division Information and Technologies services including the Internet should be familiar with:

- Copyright laws as they apply to software and electronic forms of information,
- The Canadian Criminal Code
<http://laws.justice.gc.ca/en/C-46/text.html>
- Applicable libel and slander laws,
- Community Net's Security Policy.
- SANS (www.sans.org)
- CERT (www.cert.org)
- Existing user group policies

Appendix "B"

E-mail

Users must not attempt to read another person's e-mail unless otherwise authorized. The e-mail system is a function of Community Net EDUVPN and the Northwest School Division's Information and Technologies infrastructure. Users should have no reasonable expectation of privacy in e-mail transmitted, received and stored on and/or through the system.

Many users access e-mail through web-based accounts hosted on external commercial sites such as user@hotmail.com, user@msn.com, or other free/commercial web based e-mail services. Because irresponsible use of web-based e-mail may compromise Community Net EDUVPN services, permission to access web-based e-mail from within the NWSD network will be limited to board approved e-mail services including mail@nwsd.ca, @sasktel.net, and @gaggle.net e-mail systems.

Appendix "C"

Games/Multimedia

Using the Northwest School Division infrastructure to access games or multimedia services for non-educational purposes is an unacceptable use of a valuable resource and is not permitted.

Appendix "D"**NOTEBOOK COMPUTERS:**

Notebook computers that have access to Northwest School Division computer systems must be secured appropriately to prevent a security risk in the event of loss or theft.

Appendix "E"**REMOTE ACCESS**

Information regarding remote access to Northwest School Division computer systems must be held confidential. Remote access instructions, dialup phone numbers and other similar information, must NOT be posted on electronic bulletin boards, listed in telephone directories, or otherwise revealed to unauthorized parties.

Appendix "F"**ANTI-VIRUS:**

Users shall not introduce a virus of any type to any Northwest School Division computer systems. All users are responsible for the protection of computer systems from computer viruses. Individual users must use extreme caution when accessing any external data, diskette, files or programs intended to be stored on Northwest School Division computers.

Appendix "G"**FILE SHARING:**

Unauthorized distribution/access of copyrighted works and noneducational material including, but not limited to audio, video or program files through Peer-to-Peer programs (e.g., Kazaa, WinMX, eDonkey, LimeWire etc.) is not permitted.

Appendix "H"

Acceptable/Incidental/Unacceptable Usage

	ACCEPTABLE		INCIDENTAL		UNACCEPTABLE		
	Acceptable	Acceptable/ Incidental	Incidental	Incidental/ Unacceptable	Unacceptable	Unacceptable (contravenes other Policies) *	Illegal
Stand Alone Computer	Word Processing. Doing the budget.		Preparing a roster for your children's soccer team over the lunch hour.	Preparing a roster for your child's soccer team, tying up the computer when co-workers need access.	Crashing the computer by installing a graphics-intensive multi-player combat game.	Excessive personal use of the computer.	Running a pirated version of a popular program on the computer.
Networked Computer	Sending an e-mail to all division technical coordinators with minutes of a meeting.		E-mails to co-workers with birthday wishes, holiday greetings.	Sending Division-wide e-mails with 'puppies 4 sale' type messages.	Distributing chain e-mail with large executable file attachments that waste limited network resources and may contain viruses.	Distributing racist or obscene jokes, pictures or graphics via e-mail.	Making a libelous statement about a co-worker or student in an e-mail.
Networked Computer on the Internet	Researching the latest developments in a topic with a class of students using the Internet.	An e-mail to a colleague deals with work and the schedule for your up-coming hockey tournament.	Browsing a news site during the lunch hour to keep up with world events.	Subscribing to a newsgroup on a government internet account that is of a personal nature.	Downloading a beta version of a program and installing it without authorization. Downloading racist, sexist, or pornographic material	Excessive personal use of work on the Internet.	Downloading, storing distributing and selling child pornography.

Note: These are examples only and not exhaustive or inclusive.



Northwest School Division Computer Network Acceptable Usage Policy

After reading *Northwest School Division Computer Network Acceptable Use Policy*, please sign the form below and return it to your administrator. The signature of the employee is mandatory before access is granted for use of the Internet by that employee.

To Be Completed by the Employee

Name of Employee: _____

Place of Employment: _____

I have read *Northwest School Division Computer Network Acceptable Use Policy*. I understand that the network services are intended for educational and administrative purposes. I understand that any other use is in violation of the policy.

The Northwest School Division has taken and will continue to take all reasonable precautions to eliminate controversial material from its network system. However, I also recognize it is impossible for the division to restrict access to all controversial material that exists outside its network and I will not hold the Northwest School Division responsible for material acquired via its network.

Employee Signature: _____

Date: _____

This form should be completed and forwarded to the Division Office where it will be placed in the employee's personnel file.