Kelsey School Division Box 4700 The Pas, MB R9A 1R4	**Code: IJND**

INTERNET TECHNOLOGY ACCEPTABLE USE

A. Purpose

This policy outlines the acceptable use of computer equipment at Kelsey School Division. The policy applies to employees, support staff, consultants, temporaries, and other workers at Kelsey School Division including all personnel affiliated with third parties and to all equipment that is owned or leased by Kelsey School Division. The use of Kelsey School Division internet technology and network is intended for responsible educational or research purposes. Access is a privilege and not a right.

B. General Use and Ownership

1. All data created on the Kelsey School Division systems remains the property of Kelsey School Division. Because of the need to protect Kelsey School Division's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to Kelsey School Division.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Kelsey School Division network accounts will be used only by the authorized owner of the account. Account holders are responsible for their passwords and all activity within their accounts. Information on acceptable use will be provided.

3. For security and network maintenance purposes, authorized individuals may monitor equipment systems and network traffic at any time.

4. Kelsey School Division reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5. Kelsey School Division computers are the property of the employer. Should an employee wish to have a private means of accessing their personal email accounts/other communication, including any access to the internet for personal reasons, employees ought to do so utilizing their own electronic device and not through a connection to the employer's network.

C. Security and Proprietary Information

1. The information contained on Kelsey School Division Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Employees should take all necessary steps to prevent unauthorized access to information of a confidential nature.

2. Authorized users are responsible for the security of their passwords and accounts.

3. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse codes.

4. Employees must use extreme caution when sending any e-mail from inside Kelsey School Division to an outside network in order to prevent the unauthorized or inadvertent disclosure of sensitive or personal information.

5. All employees are responsible for ensuring periodic review and clean-up of their individual e-mail files to avoid undue overload on the system.

D. Unacceptable Use

1. Under no circumstances may Kelsey School Division-owned resources be used to engage in any activity deemed illegal under provincial, federal or international law.

2. Other prohibited activities include:

a) Violating the rights of any person, organization or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.

b) Unauthorized copying of copyrighted material including installation of any copyrighted software for which Kelsey School Division or the end user does not have an active license.

c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

d) Introducing malicious programs into the network or server (eg., viruses, worms, Trojan horses, e-mail bombs, spyware, etc.). No one shall reconfigure network software or operating systems or install or download software on any computer system or stand-alone computer without the written authorization of the Computer Systems Administrator, the Secretary Treasurer or the Superintendent.

e) Revealing an account password to others or allowing use of an account by others. This includes family and other household members when work is being done at home.

f) Using a Kelsey School Division computing asset to actively engage in procuring or transmitting material that is in violation with sexual harassment or hostile workplace laws in the user's local jurisdiction.

g) Making fraudulent offers of products, items, or services originating from any Kelsey School Division account.

h) Making statements about commitments/guarantees, expressly or implied, unless it is a part of normal job duties.

i) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's host computer, via any means locally or via the Internet/Intranet/Extranet.

j) Providing information about Kelsey School Division employees to parties outside Kelsey School Division.

E. Prohibited E-mail and Communications Activities:

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forgoing, of e-mail header information.

4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "pyramid" schemes of any type.

6. Use of unsolicited e-mail originating from within Kelsey School Division networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Kelsey School Division or connected via Kelsey School Division network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8. Users are prohibited from accessing, uploading, downloading or distributing material that the school has determined to be objectionable using school division network technology or personal communication devices such as digital cameras and cell phones (including those equipped with digital cameras).

F. Guidelines on Anti-Virus Process

Users are directed to:

1. Always run the Kelsey School Division standard supported anti-virus software. Download and install anti-virus software updates as they become available (typically this process is automated).

2. NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

3. Delete spam, chain, and other junk e-mail without forwarding.

4. Never download files from unknown or suspicious sources.

5. Avoid direct disk sharing with read/write access unless there is absolutely a requirement to do so.

6. Always scan a file from an unknown portable source for viruses before using it.

7. Back-up critical data and system configurations on a regular basis and store the data in a safe place.

8. If the anti-virus software is disabled, do not run any applications that could transfer a virus, eg., e-mail or file sharing.

G. Sanctions

1. Any malicious attempt to harm or destroy hardware, software, or data belonging to Kelsey School Division or any other account holder will result in cancellation of Kelsey School Division network privileges.

2. Users may not violate, or attempt to violate, the security of the Kelsey School Division computers, data, or network. Any user who exhibits inappropriate behavior will be subject to appropriate discipline, which may include loss of user privileges, suspensions, expulsion or legal action.

3. Administrators reserve the right to suspend or terminate a user's access to the Kelsey School Division network upon any breach of the Kelsey School Division Acceptable Use Policy by the user. Appeals may be made to the school administration or via collective agreement processes.